ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28456—2012

IPsec 协议应用测试规范

Testing specification for applications of IPsec protocol

2012-06-29 发布　　2012-10-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:信息工程大学信息工程学院。

本标准主要起草人:曾勇军、王清贤、颜学雄、武东英、朱俊虎、尹美娟。

引　言

IPsec 是目前广泛使用的网络安全协议，相关产品种类较多。尽管各厂家均声称支持 IPsec 协议，但由于协议理解上的不同，造成产品在实现方式、完成的功能、提供的安全服务上存在差异。此外目前缺少规范的评估和检测手段，难以确定 IPsec 协议应用与协议标准的符合程度，难以给出产品准确的评价和分类，这不利于 IPsec 协议的推广和使用。为进一步规范 IPsec 协议的开发、评估和使用，有必要对 IPsec 协议的测试标准进行研究和制定。

本标准为 IPsec 协议应用的测试标准，依据 IPsec 协议相关 RFC 标准制定。

本标准根据 IPsec 协议的工作模式，从功能、性能、健壮性和互操作性等方面组织测试内容并设计测试步骤。本标准给出的测试步骤，旨在规范测试基本步骤和关键要点，测试人员可在此基础上选择相关的辅助工具，产生具体的测试用例并进行测试。

IPsec 协议应用测试规范

1 范围

本标准对 IPsec 协议应用的测试内容及测试步骤进行了规范。

本标准适用于 IPsec 协议应用的开发单位、第三方授权测试认证机构、用户等对 IPsec 协议应用测试时参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8—2001 信息技术 词汇 第 8 部分：安全

GB/T 17178.1—1997 信息技术 开放系统互连 一致性测试方法和框架 第 1 部分：基本概念

3 术语和定义

GB/T 5271.8—2001 界定的以及下列术语和定义适用于本文件。

3.1

IP 安全协议 IP security

一套用于保护 IP 通信的安全协议。它是 IPv4 的一个可选协议系列，也是 IPv6 的组成部分之一，是一个网络层协议。它提供了认证和加密两种安全机制：认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到篡改；加密机制通过对数据进行编码来保证数据的保密性，防止数据在传输过程中遭到截获而失密。

3.2

IPsec 协议应用 application of the IPsec protocol

按照 IPsec 协议标准实现的产品或功能模块。

3.3

安全关联 security association

两个通信实体经协商建立起来的一种协定，它描述了实体如何利用安全服务来进行安全的通信。安全关联包括了执行各种网络安全服务所需要的信息。

3.4

互联网安全关联与密钥管理协议 internet security association and key management protocol

定义了建立、协商、修改和删除安全关联的过程和报文格式，并定义了交换密钥产生和认证数据的载荷格式。这些格式为传输密钥和认证信息提供了一致的框架。

3.5

载荷 payload

ISAKMP 通信双方交换信息的传输形式，是构造 ISAKMP 消息的基本单位。

3.6

认证头 authentication header

属于 IPsec 的一种协议，用于提供 IP 数据报的数据完整性、数据源认证以及抗重放攻击服务的功能。

3.7

封装安全载荷　escapsulating security payload

属于 IPsec 的一种协议，用于提供 IP 数据报的保密性、数据完整性、数据源认证以及抗重放攻击服务的功能。

3.8

互联网密钥交换　internet key exchange

定义了协商 IPsec 协议参数的密钥交换架构，用于生成经过鉴定的密钥材料。

3.9

传输模式　transport mode

IPsec 保护的是网络层以上数据。在这种模式中，IPsec 会拦截从上层到网络层的数据，并根据具体的配置提供安全保护。

3.10

传输邻接模式　transport adjacency mode

IPsec 安全关联的一种组合模式，对同一个 IP 数据报使用多于一个传输模式的安全协议。

3.11

隧道模式　tunnel mode

IPsec 保护的是整个 IP 数据报。在这种模式中，IPsec 会拦截内部网络传递的数据，并根据具体的配置提供安全保护。

3.12

迭代隧道模式　iterated tunneling mode

IPsec 安全关联的一种组合模式，对同一个 IP 数据报使用多于一个隧道模式的安全协议。

3.13

主机　host

数据报文的始发设备或终结设备，可作为端的安全服务提供者，为自身的通信提供安全服务。

3.14

安全网关　security gateway

实现 IPsec 的中间设备，为内部主机之间的通信提供安全服务。

3.15

主模式交换　main mode exchange

由互联网密钥交换(IKE)协议所定义的一种交换方式，用于协商建立互联网安全关联和密钥管理协议的安全关联(ISAKMP SA)。该交换方式可提供身份保护，是互联网安全关联和密钥管理协议(ISAKMP)所定义的身份保护交换的实例。

3.16

野蛮模式交换　aggressive mode exchange

由互联网密钥交换(IKE)协议所定义的一种交换方式，用于协商建立互联网安全关联和密钥管理协议的安全关联(ISAKMP SA)。该交换方式不提供身份保护，是互联网安全关联和密钥管理协议(ISAKMP)所定义的野蛮模式交换的实例。

3.17

快速模式交换　quick mode exchange

由互联网密钥交换(IKE)协议所定义的一种交换方式，用于在互联网安全关联和密钥管理协议的安全关联(ISAKMP SA)的保护下，协商建立 IP 安全协议的安全关联(IPsec SA)。

3.18

ISAKMP 信息交换　ISAKMP informational exchange

由互联网密钥交换(IKE)协议所定义的一种辅助性交换,必须在互联网安全关联和密钥管理协议的安全关联(ISAKMP SA)的保护下,用来传送通知或消息。

3.19

初始交换　initial exchange

由互联网密钥交换协议版本 2(IKEv2)定义的一种交换方式,用于创建互联网密钥交换协议的安全关联(IKE SA)和子安全关联(CHILD SA)。

3.20

CREATE_CHILD_SA 交换　CREATE_CHILD_SA exchange

由互联网密钥交换协议版本 2(IKEv2)定义的一种交换方式,用于创建子安全关联(CHILD SA)。

3.21

功能测试　function testing

测试 IPsec 协议应用的基本功能,包括身份认证功能、数据保密性保护功能和数据完整性保护功能。

3.22

性能测试　performance testing

测试在不同的网络负载情况下 IPsec 协议应用的性能参数。

3.23

健壮性测试　robustness testing

测试 IPsec 协议应用对错误(包括无效的、高强度输入、非期望输入或者恶意攻击)的有效处理能力。

3.24

互操作性测试　interoperability testing

测试不同 IPsec 协议应用之间的互操作能力。

3.25

基本互连测试　basic interconnection testing

测试 IPsec 协议应用的基本互连互通的情况,这是其他测试的基础。

3.26

行为测试　behaviour testing

测试 IPsec 协议应用的动态一致性,包括正确行为符合性测试和非正确行为符合性测试。

3.27

连接建立时延　connection established delay

从连接建立请求开始,到连接建立完成所经过的时间。

3.28

传送时延　transmission delay

数据从一方传送到另一方的时间。

3.29

连接拆除时延　connection released delay

连接释放需要的时间。连接拆除包括两种类型,一是服务的请求者完成服务后,主动请求拆除连接的时延,二是服务的提供者主动拆除连接的时延。

3.30

吞吐量　throughput

丢包率为零的情况下，单位时间内传输有效数据的数量。

3.31

剩余错误比率　residual error ratio

在给定的时间间隔内，传送不正确、丢失或者重复的数据量与传输正确的数据量之比。

3.32

失败概率　probability of failure

包括连接建立失败概率、传送失败概率以及连接拆除失败概率等。

4　缩略语

AH	认证头	Authentication Header
CPU	中央处理单元	Central Processor Unit
DOI	解释域	Domain Of Interpreter
DUT	被测设备	Device Under Tester
ESP	封装安全载荷	Escapsulating Security Payload
HMAC	散列消息认证码	Hash Message Authentication Code
ICMP	因特网控制报文协议	Inernet Control Message Protocol
ICV	完整性校验值	Integrity Check Value
IKE	因特网密钥交换协议	Internet Key Exchange
IKEv1	因特网密钥交换协议版本 1	Internet Key Exchange v1
IEKv2	因特网密钥交换协议版本 2	Internet Key Exchange v2
IP	因特网协议	Internet Protocol
IPsec	IP 安全协议	IP security
ISAKMP	因特网安全关联与密钥管理协议	Internet Security Association and Key Management Protocol
IV	初始化向量	Initialization Vector
MAC	消息认证码	Message Authentication Code
NAT	网络地址翻译	Network Address Translation
MTU	最大传送单元	Maximun Transmission Unit
PFS	完美前向保密	Perfect Forward Secrecy
PRF	伪随机函数	Pseudo-Random Function
SA	安全关联	Security Association
SAD	安全关联数据库	Security Association Database
SG	安全网关	Security Gateway
SPD	安全策略数据库	Security Policy Database
SPI	安全参数索引	Security Parameter Index

5　测试说明

5.1　测试对象说明

本标准是 IPsec 协议的测试标准，测试对象为依据 RFC 相关标准实现的 IPsec 协议应用。

IPsec 协议应用可提供基于密码的安全服务，使用的密码算法和密钥管理策略应符合国家密码主管部门的有关规定。

IPsec 协议描述可见附录 A，附录 B 和附录 C 给出了 IKEv1 和 IKEv2 的密钥交换机制。

5.2 测试内容说明

本标准定义了 IPsec 协议应用的测试内容，包括功能测试、性能测试、健壮性测试和互操作性测试。

功能测试用于测试 IPsec 协议应用实现的基本功能，包括基本互连测试、安全功能测试和行为测试。基本互连测试用于测试 IPsec 协议应用的连通情况，是其他测试的基础；安全功能测试完成 IPsec 协议应用的各项安全功能测试，包括密码算法协商、身份认证、数据保密性和数据完整性等；为保证各项安全功能的有效性，IPsec 协议应用的动态行为必须符合协议规范要求，行为测试完成 IPsec 协议应用的动态行为的符合性测试，包括正确输入行为符合性测试和非正确输入行为符合性测试。

性能测试用于测试在不同的网络负载情况下 IPsec 协议应用的性能参数，包括连接建立时延、传送时延、连接拆除时延、单位时间新建连接数、设备支持的总连接数、加解密时延、吞吐量、剩余错误比率以及失败概率等。

健壮性测试用于测试 IPsec 协议应用在无效数据输入或在高强度负载环境下，各项功能保持正确运行的程度，即测试 IPsec 协议应用对错误的有效处理能力，主要包括无效报文处理能力、异常事件处理能力和高强度负载下的处理能力。IPsec 协议应用属于安全产品，其健壮性对于安全功能的有效性至关重要，因此本标准对该质量属性进行了测试。

互操作性测试用于完成不同 IPsec 协议应用之间的互操作能力测试，包括基本互连互操作性测试和安全功能互操作测试。基本互连互操作性测试内容和功能测试中的基本互连测试内容一样，安全功能互操作性测试和功能测试中的安全功能测试内容一样，主要区别在于功能测试是 IPsec 协议应用和测试系统之间的交互，而互操作性测试是不同的 IPsec 协议应用间的交互。

5.3 测试环境说明

本标准推荐采用 GB/T 17178.1— 1997 中的远程测试方法，构造测试环境并给出相关的测试步骤。IPsec 协议应用测试的典型网络拓扑结构如图 1 所示。

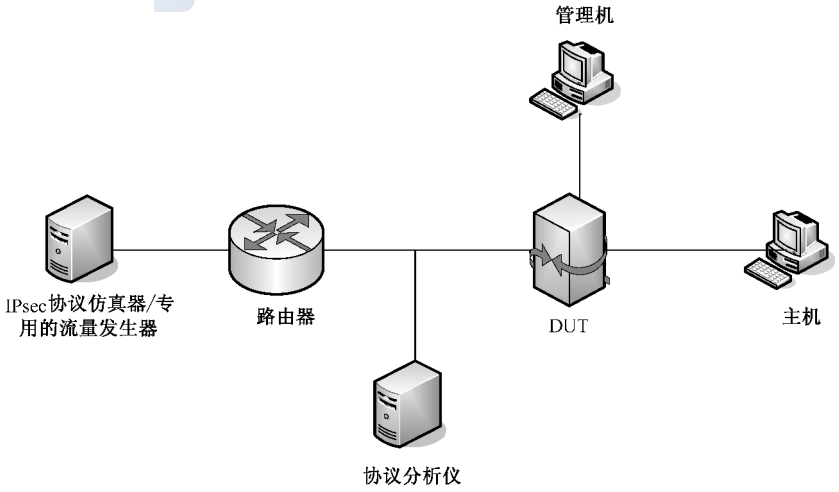


图 1 IPsec 协议应用测试的网络拓扑结构图

上述拓扑结构可根据待测设备 DUT 的类型（如终端或网关）灵活配置，如内部主机和管理机在终端情况下可不出现。

测试工具包括但不限于：IPsec 协议仿真器用于模拟 IPsec 协议的动作并进行测试；专用的流量发

生器用于测试 DUT 的性能;协议分析仪实现数据报的分析、存储和重放等。

6 测试内容

6.1 AH 传输模式测试内容

6.1.1 功能测试内容

6.1.1.1 基本互连测试

测试 IPsec 协议应用在 AH 传输模式下的基本连通能力。

6.1.1.2 安全功能测试

测试 IPsec 协议应用在 AH 传输模式下的安全功能,测试内容包括:

a) AH 传输模式功能:能够支持 AH 传输模式,建立 AH 传输模式的 SA 并进行通信;
b) 数据完整性保护功能:能够支持数据完整性保护功能,及时发现篡改、删除等情况的发生;
c) 数据源认证功能:能够支持数据源认证功能,及时发现伪造、欺骗等情况的发生;
d) 抗重放攻击服务功能:能够支持抗重放攻击服务功能,可检测出重放的报文并丢弃;
e) 应用 IPsec 策略功能:能够配置 SPD 支持应用 IPsec 策略功能,允许合法的业务通过时获得 AH 协议的保护;
f) 旁路策略功能:能够配置 SPD 支持旁路策略功能,允许合法的业务通过时不使用 AH 协议的保护;
g) 丢弃策略功能:能够配置 SPD 支持丢弃策略功能,不合法的业务通过时将被丢弃;
h) SPD 策略选择功能:能够配置多个 SPD 策略实体,在发送或接收分组时,可选择合适的 SPD 策略进行处理;
i) SA 生存期测试功能:能够支持 SA 的有效生存期管理功能,防止利用过期的 SA 传递数据;
j) 分片重组功能:能够支持分片重组功能,确保数据通过网络传递和接收时得到正确的处理;
k) 序号增长功能:能够支持数据报文序号的自动递增功能。

6.1.2 性能测试内容

测试 IPsec 协议应用在 AH 传输模式下的性能,测试内容包括:

a) 吞吐量:测量在以太网长帧和短帧时,IPsec 协议应用的数据吞吐量;
b) 传送时延:测量 IPsec 协议应用的数据传送时延;
c) 剩余错误比率:测量 IPsec 协议应用的剩余错误比率;
d) 失败概率:测量 IPsec 协议应用传送失败的概率。

6.1.3 健壮性测试内容

6.1.3.1 无效报文处理能力

测试 IPsec 协议应用在 AH 传输模式下的无效报文处理能力,测试内容包括:

a) 错误报文处理能力:测试接收到 AH 传输模式封装的报文中有错误时,IPsec 协议应用处理能力。常见的错误报文如 AH 头部中保留字段不为 0、SPI 在 0～255 之间、序号为 0、ICV 字段不正确等。
b) 非期望报文处理能力:测试接收到一个非期望的 AH 传输模式封装的报文时,IPsec 协议应用处理能力。常见的非期望报文如序号不在接受窗口内、重复报文等。

6.1.3.2 异常事件处理能力

测试 IPsec 协议应用在 AH 传输模式下的异常事件处理能力，测试内容包括：

a) 连接中断处理能力：测试在网络物理连接突然非正常中断时，IPsec 协议应用的处理能力；

b) 无效 SA 处理能力：测试接收到 AH 传输模式封装的报文，但没有有效的 SA 时，IPsec 协议应用的处理能力。

6.1.3.3 高强度负载处理能力

测试 IPsec 协议应用在 AH 传输模式下的高强度负载处理能力，测试内容包括：

a) 网络高强度负载处理能力：测试在网络流量负载比较大时，IPsec 协议应用的处理能力；

b) 系统高强度负载处理能力：测试在多种资源(如 CPU 或者内存)消耗比较多时，IPsec 协议应用的处理能力。

6.1.4 互操作性测试内容

6.1.4.1 基本互连测试

测试不同 IPsec 协议应用在 AH 传输模式下的基本连通能力。

6.1.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 AH 传输模式下的功能互操作情况。测试内容见 6.1.1.2 的规定。

6.2 AH 隧道模式测试内容

6.2.1 功能测试内容

6.2.1.1 基本互连测试

测试 IPsec 协议应用在 AH 隧道模式下的基本连通能力。

6.2.1.2 安全功能测试

测试 IPsec 协议应用在 AH 隧道模式下支持的安全功能。测试内容见 6.1.1.2 的规定。

6.2.2 性能测试内容

测试 IPsec 协议应用在 AH 隧道模式下的性能指标。测试内容见 6.1.2 的规定。

6.2.3 健壮性测试内容

6.2.3.1 无效报文处理能力

测试 IPsec 协议应用在 AH 隧道模式下无效报文处理能力。测试内容见 6.1.3.1 的规定。

6.2.3.2 异常事件处理能力

测试 IPsec 协议应用在 AH 隧道模式下异常事件处理能力。测试内容见 6.1.3.2 的规定。

6.2.3.3 高强度负载处理能力

测试 IPsec 协议应用在 AH 隧道模式下高强度负载处理能力。测试内容见 6.1.3.3 的规定。

6.2.4 互操作性测试内容

6.2.4.1 基本互连测试

测试不同 IPsec 协议应用在 AH 隧道模式下的基本连通能力。

6.2.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 AH 隧道模式下的功能互操作情况。测试内容见 6.1.1.2 的规定。

6.3 ESP 传输模式测试内容

6.3.1 功能测试内容

6.3.1.1 基本互连测试

测试 IPsec 协议应用在 ESP 传输模式下的基本连通能力。

6.3.1.2 安全功能测试

测试 IPsec 协议应用在 ESP 传输模式下的安全功能，测试内容包括：

a) ESP 传输模式功能：能够支持 ESP 传输模式，建立 ESP 传输模式的 SA 并进行通信；
b) 数据完整性保护功能：能够支持数据完整性保护功能，及时发现篡改、删除等情况的发生；
c) 数据源认证功能：能够支持数据源认证功能，及时发现伪造、欺骗等情况的发生；
d) 数据保密性功能：能够支持数据保密性功能，防止数据传输过程中的非授权泄露；
e) 抗重放攻击服务功能：能够支持抗重放攻击服务功能，可检测出重放的报文并丢弃；
f) 应用 IPsec 策略功能：能够配置 SPD 支持应用 IPsec 策略功能，允许合法的业务通过时获得 ESP 协议的保护；
g) 旁路策略功能：能够配置 SPD 支持旁路策略功能，允许合法的业务通过时不使用 ESP 协议的保护；
h) 丢弃策略功能：能够配置 SPD 支持丢弃策略功能，不合法的业务通过时将被丢弃；
i) SPD 策略选择功能：能够配置多个 SPD 策略实体，在发送或接收分组时，可选择合适的 SPD 策略进行处理；
j) SA 生存期测试功能：能够支持 SA 的有效生存期管理功能，防止利用过期的 SA 传递数据；
k) 分片重组功能：能够支持分片重组功能，确保数据通过网络传递和接收时得到正确的处理；
l) 序号增长功能：能够支持发送数据报文序号的自动递增功能；
m) NAT 穿越功能：能够支持 NAT 穿越功能，满足 IPsec 与 NAT 的兼容性要求。

6.3.2 性能测试要求

测试 IPsec 协议应用在 ESP 传输模式下的性能，测试内容包括：

a) 加解密吞吐量：测量在以太网长帧和短帧时，IPsec 协议应用在丢包率为 0 的条件下内部接口上达到的双向数据最大流量；
b) 加解密时延：测量在以太网长帧和短帧时，IPsec 协议应用在丢包率为 0 的条件下，一个报文经过加密算法计算变为密文，再由密文解密还原为明文所消耗的平均时间；
c) 传送时延：测量 IPsec 协议应用的数据传送时延；
d) 剩余错误比率：测量 IPsec 协议应用的剩余错误比率；
e) 失败概率：测量 IPsec 协议应用传送失败的概率。

6.3.3 健壮性测试内容

6.3.3.1 无效报文处理能力

测试 IPsec 协议应用在 ESP 传输模式下的无效报文处理能力，测试内容包括：

a) 错误报文处理能力：测试接收到 ESP 传输模式封装的报文中有错误时，IPsec 协议应用的处理能力。常见的错误报文如 SPI 在 0～255 之间、序号为 0、填充长度和下一个头字段不以 4 字节对齐、填充长度不在 0～255 之间、载荷长度为 0、ICV 字段不正确等。

b) 非期望报文处理能力：测试接收到一个非期望的 ESP 传输模式封装的报文时，IPsec 协议应用的处理能力。常见的非期望报文如序号不在接受窗口内、重复报文等。

6.3.3.2 异常事件处理能力

测试 IPsec 协议应用在 ESP 传输模式下的异常事件处理能力，测试内容包括：

a) 连接中断处理能力：测试在网络物理连接突然非正常中断时，IPsec 协议应用处理能力；

b) 无效 SA 处理能力：测试接收到 ESP 传输模式封装的报文，但没有有效的 SA 时，IPsec 协议应用处理能力。

6.3.3.3 高强度负载处理能力

测试 IPsec 协议应用在 ESP 传输模式下的高强度负载处理能力，测试内容包括：

a) 网络高强度负载处理能力：测试在网络流量负载比较大时，IPsec 协议应用处理能力；

b) 系统高强度负载处理能力：测试在多种资源（如 CPU 或者内存）消耗比较多时，IPsec 协议应用处理能力。

6.3.4 互操作性测试内容

6.3.4.1 基本互连测试

测试不同 IPsec 协议应用在 ESP 传输模式下的基本连通能力。

6.3.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 ESP 传输模式下的功能互操作情况。测试内容见 6.3.1.2 的规定。

6.4 ESP 隧道模式测试内容

6.4.1 功能测试内容

6.4.1.1 基本互连测试

测试 IPsec 协议应用在 ESP 隧道模式下的基本连通能力。

6.4.1.2 安全功能测试

测试 IPsec 协议应用在 ESP 隧道模式下的安全功能，测试内容包括：

a) 基本安全功能：测试 IPsec 协议应用在 ESP 隧道模式下支持的各种安全功能。测试内容见 6.3.1.2的规定。

b) 有限业务流的保密性保护功能：能够支持有限业务流的保密性保护功能，防止对报文内容的分析。

6.4.2 性能测试内容

测试 IPsec 协议应用在 ESP 隧道模式下的各种性能指标。测试内容见 6.3.2 的规定。

6.4.3 健壮性测试内容

6.4.3.1 无效报文处理能力

测试 IPsec 协议应用在 ESP 隧道模式下无效报文处理能力。测试内容见 6.3.3.1 的规定。

6.4.3.2 异常事件处理能力

测试 IPsec 协议应用在 ESP 隧道模式下异常事件处理能力。测试内容见 6.3.3.2 的规定。

6.4.3.3 高强度负载处理能力

测试 IPsec 协议应用在 ESP 隧道模式下高强度负载处理能力。测试内容见 6.3.3.3 的规定。

6.4.4 互操作性测试内容

6.4.4.1 基本互连测试

测试不同 IPsec 协议应用在 ESP 隧道模式下的基本连通能力。

6.4.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 ESP 隧道模式下的功能互操作情况。测试内容见 6.4.1.2 的规定。

6.5 传输邻接模式测试内容

6.5.1 功能测试内容

6.5.1.1 基本互连测试

测试 IPsec 协议应用在传输邻接模式下的基本连通能力。

6.5.1.2 安全功能测试

测试 IPsec 协议应用在传输邻接模式下的安全功能，测试内容包括：

a) 传输邻接模式功能：能够支持传输邻接模式，建立传输邻接模式的 SA 并进行通信；
b) 数据完整性保护功能：能够支持数据完整性保护功能，及时发现篡改、删除等情况的发生；
c) 数据源认证功能：能够支持数据源认证功能，及时发现伪造、欺骗等情况的发生；
d) 数据保密性功能：能够支持数据保密性保护功能，防止数据传输过程中的非授权泄露；
e) 抗重放攻击服务功能：能够支持抗重放攻击服务功能，可检测出重放的报文并丢弃；
f) 应用 IPsec 策略功能：能够配置 SPD 支持应用 IPsec 策略功能，允许合法的业务通过时获得安全性保护；
g) 旁路策略功能：能够配置 SPD 支持旁路策略功能，允许合法的业务通过时不使用安全性保护；
h) 丢弃策略功能：能够配置 SPD 支持丢弃策略功能，不合法的业务通过时将被丢弃；
i) SPD 策略选择功能：能够配置多个 SPD 策略实体，在发送或接收分组时，可选择合适的 SPD 策略进行处理；
j) SA 生存期测试功能：能够支持 SA 的有效生存期管理功能，防止利用过期的 SA 传递数据；
k) 分片重组功能：能够支持分片重组功能，确保数据通过网络传递和接收时得到正确的处理；

l) 序号增长功能：IPsec 协议应用支持发送数据报文序号的自动递增功能。

6.5.2 性能测试内容

测试 IPsec 协议应用在传输邻接模式下的各种性能指标，测试内容见 6.3.2 的规定。

6.5.3 健壮性测试内容

6.5.3.1 无效报文处理能力

测试 IPsec 协议应用在传输邻接模式下的无效报文处理能力，测试内容包括：

a) 错误报文处理能力：测试接收到传输邻接模式封装的报文中有错误时，IPsec 协议应用处理能力。常见的错误报文如 AH 头部中保留字段不为 0、SPI 在 0～255 之间、序号为 0、ICV 字段不正确，ESP 封装结构中 SPI 在 0～255 之间、序号为 0、填充长度和下一个头字段不以 4 字节对齐、填充长度不在 0～255 之间、载荷长度为 0 等。

b) 非期望报文处理能力：测试接收到一个非期望的传输邻接模式封装的报文时，IPsec 协议应用处理能力。常见的非期望报文如序号不在接受窗口内、重复报文等。

6.5.3.2 异常事件处理能力

测试 IPsec 协议应用在传输邻接模式下的异常事件处理能力，测试内容包括：

a) 连接中断处理能力：测试在网络物理连接突然非正常中断时，IPsec 协议应用处理能力；

b) 无效 SA 处理能力：测试接收到传输邻接模式封装的报文，但没有有效的 SA 时，IPsec 协议应用处理能力。

6.5.3.3 高强度负载处理能力

测试 IPsec 协议应用在传输邻接模式下的高强度负载处理能力，测试内容包括：

a) 网络高强度负载处理能力：测试在网络流量负载比较大时，IPsec 协议应用处理能力；

b) 系统高强度负载处理能力：测试在多种资源（如 CPU 或者内存）消耗比较多时，IPsec 协议应用处理能力。

6.5.4 互操作性测试内容

6.5.4.1 基本互连测试

测试不同 IPsec 协议应用在传输邻接模式下的基本连通能力。

6.5.4.2 功能互操作性测试

测试不同 IPsec 协议应用在传输邻接模式下的功能互操作情况。测试内容见 6.5.1.2 的规定。

6.6 迭代隧道模式测试内容

6.6.1 功能测试内容

6.6.1.1 基本互连测试

测试 IPsec 协议应用在迭代隧道模式下的基本连通能力。

6.6.1.2 安全功能测试

测试 IPsec 协议应用在迭代隧道模式下的安全功能，测试内容包括：

a) 迭代隧道模式功能：能够支持迭代隧道模式，建立迭代隧道模式的 SA 并进行通信；
b) 数据完整性保护功能：能够支持数据完整性保护功能，及时发现篡改、删除等情况的发生；
c) 数据源认证功能：能够支持数据源认证功能，及时发现伪造、欺骗等情况的发生；
d) 数据保密性功能：能够支持数据保密性保护功能，防止数据传输过程中的非授权泄露；
e) 有限业务流的保密性保护功能：能够支持有限业务流的保密性保护功能，防止对报文内容的分析；
f) 抗重放攻击服务功能：能够支持抗重放攻击服务功能，可检测出重放的报文并丢弃；
g) 应用 IPsec 策略功能：能够配置 SPD 支持应用 IPsec 策略功能，允许合法的业务通过时获得安全性保护；
h) 旁路策略功能：能够配置 SPD 支持旁路策略功能，允许合法的业务通过时不使用安全性保护；
i) 丢弃策略功能：能够配置 SPD 支持丢弃策略功能，不合法的业务通过时将被丢弃；
j) SPD 策略选择功能：能够配置多个 SPD 策略实体，在发送或接收分组时，可选择合适的 SPD 策略进行处理；
k) SA 生存期测试功能：能够支持 SA 的有效生存期管理功能，防止利用过期的 SA 传递数据；
l) 分片重组功能：能够支持分片重组功能，确保数据通过网络传递和接收时得到正确的处理；
m) 序号增长功能：能够支持发送数据报文序号的自动递增功能。

6.6.2 性能测试内容

测试 IPsec 协议应用在迭代隧道模式下的各种性能指标。测试内容见 6.3.2 的规定。

6.6.3 健壮性测试内容

6.6.3.1 无效报文处理能力

测试 IPsec 协议应用在迭代隧道模式下无效报文处理能力。测试内容见 6.5.3.1 的规定。

6.6.3.2 异常事件处理能力

测试 IPsec 协议应用在迭代隧道模式下异常事件处理能力。测试内容见 6.5.3.2 的规定。

6.6.3.3 高强度负载处理能力

测试 IPsec 协议应用在迭代隧道模式下高强度负载处理能力。测试内容见 6.5.3.3 的规定。

6.6.4 互操作性测试内容

6.6.4.1 基本互连测试

测试不同 IPsec 协议应用在迭代隧道模式下的基本连通能力。

6.6.4.2 功能互操作性测试

测试不同 IPsec 协议应用在迭代隧道模式下的功能互操作情况。测试内容见 6.6.1.2 的规定。

6.7 IKEv1 主模式测试内容

6.7.1 功能测试内容

6.7.1.1 基本互连测试

测试在主模式交换情况下，IKEv1 协议的基本连通能力。

6.7.1.2 安全功能测试

测试在主模式交换情况下 IKEv1 协议支持的安全功能，测试内容包括：

a) 身份认证方法协商功能：能够支持身份认证方法的协商功能；
b) 身份认证协商过程：能够按照所协商的身份认证方法，完成身份的认证协商功能；
c) 加密算法协商功能：能够支持加密算法的协商功能；
d) 伪随机函数 PRF 协商功能：能够支持伪随机函数 PRF 的协商；
e) 密钥协商功能：能够支持密钥协商的功能；
f) 数据加密功能：能够应用协商好的加密算法和密钥对传输的数据进行加密保护；
g) NAT 穿越探测功能：能够探测参与方是否支持 NAT 穿越，网络中是否存在 NAT 设备；
h) NAT KEEPALIVE 功能：NAT 后的协商参与方能够定期地发送 NAT KEEPALIVE 报文，维持 NAT 映射。

6.7.1.3 发起方行为测试

在主模式交换情况下，IKEv1 发起方行为测试内容如下：

a) 初始化时发起方接收到安全协议（如 AH 或 ESP 协议）的协商请求，构造消息 1 并发送给响应方。消息 1 中包含安全关联载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。
b) 发起方接收消息 2。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 2 中承载的协商结果，构造消息 3 并发送给响应方。消息 3 中包含密钥交换载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。
c) 发起方接收消息 4。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 4 中承载的协商结果，构造消息 5 并发送给响应方。消息 5 中包含认证载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。
d) 发起方接收消息 6。验证接收到的消息的合法性：若非法，则丢弃；否则，进行解密，验证认证信息是否正确，记录消息 6 中承载的协商结果。设置协商完成标志。
e) 发起方收到删除 ISAKMP SA 请求或 ISAKMP SA 到期通知，清除连接状态。

6.7.1.4 响应方行为测试

在主模式交换情况下，IKEv1 响应方行为测试内容如下：

a) 初始化时响应方等待接收消息 1。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 1 中承载的协商请求，构造消息 2 并发送给发起方。消息 2 中包含安全关联载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。
b) 响应方接收消息 3。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 3 中承载的协商请求，构造消息 4 并发送给发起方。消息 4 中包含密钥交换载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。
c) 响应方接收消息 5。验证接收到的消息的合法性：若非法，则丢弃；否则，进行解密，验证认证信息是否正确，构造消息 6 并发送给发起方。消息 6 中包含认证载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。设置协商完成标志。
d) 响应方收到删除 ISAKMP SA 请求或 ISAKMP SA 到期通知，清除连接状态。

6.7.2 性能测试内容

测试在主模式交换情况下 IKEv1 协议的性能指标，测试内容包括：

a) 连接建立时延：测量 IKEv1 协议的阶段 1(见附录 B 的 B.2.1)连接建立时延；
b) 单位时间新建连接数：测量 IKEv1 协议每秒钟能够建立的阶段 1 连接数；
c) 设备支持的总连接数：测量 IKEv1 协议所能支持的阶段 1 连接总数；
d) 剩余错误比率：测量 IKEv1 协议协商报文的剩余错误比率；
e) 失败概率：测量 IKEv1 协议协商失败的概率，包括连接建立失败概率、传送失败概率等；
f) 密钥更新：测量 IKEv1 协议的密钥自动更新机制，如要求 ISAKMP SA 的密钥更新周期不大于 24 h。

6.7.3 健壮性测试内容

6.7.3.1 无效报文处理能力

测试在主模式交换情况下 IKEv1 协议的无效报文处理能力，测试内容包括：
a) 错误报文处理能力：测试接收到主模式交换的报文中有错误时，IKEv1 协议的处理能力；
b) 非期望报文处理能力：测试接收到非期望的主模式交换报文时，IKEv1 协议的处理能力。

6.7.3.2 异常事件处理能力

测试在主模式交换情况下 IKEv1 协议的异常事件处理能力，测试内容包括：
a) 连接中断处理能力：测试网络物理连接突然非正常中断时，IKEv1 协议的处理能力；
b) 等待超时处理能力：测试等待报文超时情况下，IKEv1 协议的处理能力。

6.7.3.3 高强度负载处理能力

测试在主模式交换情况下 IKEv1 协议的高强度负载处理能力，测试内容包括：
a) 网络高强度负载处理能力：测试在网络流量负载比较大时，IKEv1 协议的处理能力；
b) 系统高强度负载处理能力：测试在多种资源(如 CPU 或者内存)消耗比较多时，IKEv1 协议的处理能力。

6.7.4 互操作性测试内容

6.7.4.1 基本互连测试

测试不同 IPsec 协议应用在 IKEv1 主模式交换情况下的基本连通能力。

6.7.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 IKEv1 主模式交换情况下的功能互操作情况。测试内容见 6.7.1.2 各条目的规定。

6.7.4.3 行为互操作性测试

测试不同 IPsec 协议应用在 IKEv1 主模式交换情况下的行为互操作情况。测试内容见 6.7.1.3 和 6.7.1.4 的规定。

6.8 IKEv1 野蛮模式测试内容

6.8.1 功能测试内容

6.8.1.1 基本互连测试

测试在野蛮模式交换情况下，IKEv1 协议的基本连通能力。

6.8.1.2 安全功能测试

测试在野蛮模式交换情况下，IKEv1 协议支持的各种安全功能，测试内容见 6.7.1.2 的规定。

6.8.1.3 发起方行为测试

在野蛮模式交换情况下，IKEv1 发起方行为测试内容如下：

a) 初始化时发起方接收到安全协议（如 AH 或 ESP 协议）的协商请求时，构造消息 1 并发送给响应方。消息 1 中包含安全关联载荷、密钥交换载荷等，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。

b) 发起方接收消息 2。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 2 中承载的协商结果，验证响应方的身份，构造消息 3 并发送给响应方。消息 3 中包含认证载荷，其格式应满足协议规范要求，提供该消息的超时重传功能。设置协商完成标志。

c) 发起方收到删除 ISAKMP SA 请求或 ISAKMP SA 到期通知，清除连接状态。

6.8.1.4 响应方行为测试

在野蛮模式交换情况下，IKEv1 响应方行为测试内容如下：

a) 初始化时响应方等待接收消息 1。验证接收到的消息的合法性：若非法，则丢弃；否则，记录消息 1 中承载的协商内容，构造消息 2 并发送给发起方。消息 2 中包含安全关联载荷、密钥交换载荷等，其格式应满足协议规范要求，提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。

b) 响应方接收消息 3。验证接收到的消息的合法性：若非法，则丢弃；否则，验证发起方身份的合法性，若验证不通过，则丢弃该消息。若身份验证通过，则设置协商完成状态。

c) 响应方收到删除 ISAKMP SA 请求或 ISAKMP SA 到期通知，清除连接状态。

6.8.2 性能测试内容

测试在野蛮模式交换情况下，IKEv1 协议支持的各种性能指标。测试内容见 6.7.2 的规定。

6.8.3 健壮性测试内容

6.8.3.1 无效报文处理能力

测试在野蛮模式交换情况下 IKEv1 协议的无效报文处理能力。测试内容见 6.7.3.1 的规定。

6.8.3.2 异常事件处理能力

测试在野蛮模式交换情况下 IKEv1 协议的异常事件处理能力。测试内容见 6.7.3.2 的规定。

6.8.3.3 高强度负载处理能力

测试在野蛮模式交换情况下 IKEv1 协议的高强度负载处理能力。测试内容 6.7.3.2 的规定。

6.8.4 互操作性测试内容

6.8.4.1 基本互连测试

测试不同 IPsec 协议应用在 IKEv1 野蛮模式交换情况下的基本连通能力。

6.8.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 IKEv1 野蛮模式交换情况下的功能互操作情况。测试内容见 6.8.1.2

的规定。

6.8.4.3 行为互操作性测试

测试不同 IPsec 协议应用在 IKEv1 野蛮模式交换情况下的行为互操作情况。测试内容见 6.8.1.3 和 6.8.1.4 的规定。

6.9 IKEv1 快速模式测试内容

6.9.1 功能测试内容

6.9.1.1 基本互连测试

测试在快速模式交换情况下,IKEv1 协议的基本连通能力。

6.9.1.2 安全功能测试

测试在快速模式交换情况下 IKEv1 协议支持的安全功能,测试内容包括:

a) 加密算法协商功能:能够支持 IPsec 安全协议(如 ESP)的加密算法协商功能;
b) MAC 算法协商功能:能够支持 IPsec 安全协议(如 AH、ESP)的 MAC 算法协商功能;
c) 密钥协商功能:能够支持 IPsec 安全协议(如 AH、ESP)的共享密钥协商功能;
d) NAT 穿越的原始地址交换功能:能够传递构造数据报文时的原始 IP 地址,实现校验和的修正。

6.9.1.3 发起方行为测试

在快速模式交换情况下,IKEv1 发起方行为测试内容如下:

a) 发起方接收到协商指示,构造消息 1 发送给响应方。消息 1 中包含安全关联载荷、密钥交换相关载荷等,其格式应满足协议规范要求,并使用阶段 1 协商的结果进行加密保护。发起方应提供消息 1 超时重传功能。若重传次数超过指定的最大值,则终止本次协商。
b) 发起方接收消息 2。验证接收到的消息的合法性:若非法,则丢弃;否则,对消息 2 进行解密,记录消息 2 中承载的协商结果,构造消息 3 并发送给响应方。消息 3 中包含认证相关载荷,其格式应满足协议规范要求,提供该消息的超时重传功能。设置协商完成标志。
c) 发起方收到删除 IPsec SA 请求或 IPsec SA 到期通知,清除连接状态。

6.9.1.4 响应方行为测试

在快速模式交换情况下,IKEv1 响应方行为测试内容如下:

a) 响应方等待接收发起方发送过来的消息 1。验证接收到的消息的合法性:若非法,则丢弃;否则,进行解密,并记录消息 1 中承载的协商内容,构造消息 2 并发送给发起方。消息 2 中包含安全关联载荷、密钥交换相关载荷等,其格式应满足协议规范要求,提供该消息的超时重传功能。若重传次数超过指定的最大值,则终止本次协商。
b) 响应方接收消息 3。验证接收到的消息的合法性:若非法,则丢弃;否则,进行解密并验证发起方身份的合法性。若身份验证通过,则设置协商完成状态。
c) 响应方收到删除 IPsec SA 请求或 IPsec SA 到期通知,清除连接状态。

6.9.2 性能测试内容

测试在快速模式交换情况下 IKEv1 协议的性能指标,测试内容包括:

a) 连接建立时延:测量 IKEv1 协议的阶段 2(见附录 B 的 B.2.2)连接建立时延;

b) 单位时间新建连接数：测量 IKEv1 协议每秒钟能够建立的阶段 2 连接数；
c) 设备支持的总连接数：测量 IPsec 协议应用所能支持的阶段 2 连接总数；
d) 剩余错误比率：测量 IKEv1 协议协商报文的剩余错误比率；
e) 失败概率：测量 IKEv1 协议协商的失败概率，包括连接建立失败概率、传送失败概率等；
f) 密钥更新：测量 IKEv1 协议的 IPsec SA 密钥更新机制，如要求密钥更新周期不大于 1 h。

6.9.3 健壮性测试内容

6.9.3.1 无效报文处理能力

测试在快速模式交换情况下 IKEv1 协议的无效报文处理能力。测试内容见 6.7.3.1 的规定。

6.9.3.2 异常事件处理能力

测试在快速模式交换情况下 IKEv1 协议的异常事件处理能力。测试内容见 6.7.3.2 的规定。

6.9.3.3 高强度负载处理能力

测试在快速模式交换情况下 IKEv1 协议的高强度负载处理能力。测试内容见 6.7.3.3 的规定。

6.9.4 互操作性测试内容

6.9.4.1 基本互连测试

测试不同 IPsec 协议应用在 IKEv1 快速模式交换情况下的基本连通能力。

6.9.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 IKEv1 快速模式交换情况下的功能互操作情况。测试内容见 6.9.1.2 的规定。

6.9.4.3 行为互操作性测试

测试不同 IPsec 协议应用在 IKEv1 快速模式交换情况下的行为互操作情况。测试内容见 6.9.1.3 和 6.9.1.4 的规定。

6.10 IKEv2 初始交换测试内容

6.10.1 功能测试内容

6.10.1.1 基本互连测试

测试在初始交换情况下，IKEv2 协议的基本连通能力。

6.10.1.2 安全功能测试

测试在初始交换情况下 IKEv2 协议支持的各种安全功能。测试内容见 6.7.1.2 的规定。

6.10.1.3 发起方行为测试

在 IKEv2 初始交换情况下，发起方行为测试内容如下：

a) 初始化时发起方接收到安全协议（如 AH 或 ESP 协议）的协商请求，构造 IKE_SA_INIT 请求消息并发送给响应方，该消息中包含安全关联载荷、密钥交换载荷，其格式应满足协议规范要求。发起方提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。

b) 发起方接收返回的响应消息。响应消息有如下两种类型：

1) 若接收到 IKE_SA_INIT 响应消息，则验证该消息的合法性：若非法，则丢弃；否则，记录响应消息中承载的协商结果，然后构造 IKE_AUTH 请求消息并发送给响应方，该消息中包含认证载荷、安全关联载荷，其格式应满足协议规范要求，并利用协商的算法和密钥加密。发起方提供该消息的超时重传功能。若重传次数超过指定的最大值，则终止本次协商。

2) 若接收到带 Cookie 的通知载荷的响应消息，则说明响应方半打开连接超过最大值，发起方发送带 Cookie 的 IKE_SA_INIT 请求消息，该请求消息格式应满足协议规范要求。

c) 发起方接收 IKE_AUTH 响应消息。验证接收到的消息的合法性：若非法，则丢弃；否则，记录该消息中承载的协商结果，根据认证载荷结构验证身份。设置协商完成标志。

d) 发起方收到删除 IKE SA 请求或 IKE SA 到期通知，清除连接状态。

6.10.1.4 响应方行为测试

在 IKEv2 初始交换情况下，响应方行为测试内容如下：

a) 响应方等待接收 IKE_SA_INIT 请求消息。验证接收到的消息的合法性：若非法，则丢弃；否则，响应方有如下两种情况：

1) 若当前的半打开连接数目未达到门限值，则发送 IKE_SA_INIT 响应消息，说明响应方可接受发起方的连接请求。该响应消息中包含安全关联载荷、密钥交换载荷等，其格式应满足协议规范要求。

2) 若当前的半打开连接数目达到门限值，则发送带 Cookie 的通知消息。此时若接收到带 Cookie 的 IKE_SA_INIT 请求消息，则发送 IKE_SA_INIT 响应消息，可检测发起方是否合法。该响应消息格式应满足协议规范要求。

b) 响应方接收 IKE_AUTH 请求消息。验证接收到的消息的合法性：若非法，则丢弃；否则，验证发起方身份的合法性，记录消息中承载的协商请求，产生 IKE_AUTH 响应消息并发送给发起方，该消息中包含认证载荷、安全关联载荷，同时利用协商的算法和密钥进行加密封装，消息格式应满足协议规范要求。设置协商完成标志。

c) 响应方收到删除 IKE SA 请求或 IKE SA 到期通知，清除连接状态。

6.10.2 性能测试内容

测试初始交换情况下 IKEv2 协议支持的各种性能指标。测试内容见 6.7.2 的规定。

6.10.3 健壮性测试内容

6.10.3.1 无效报文处理能力

测试在初始交换情况下 IKEv2 协议的无效报文处理能力。测试内容见 6.7.3.1 的规定。

6.10.3.2 异常事件处理能力

测试在初始交换情况下 IKEv2 协议的异常事件处理能力。测试内容见 6.7.3.2 的规定。

6.10.3.3 高强度负载处理能力

测试在初始交换情况下 IKEv2 协议的高强度负载处理能力。测试内容见 6.7.3.3 的规定。

6.10.4 互操作性测试内容

6.10.4.1 基本互连测试

测试不同 IPsec 协议应用在 IKEv2 初始交换情况下的基本连通能力。

6.10.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 IKEv2 初始交换情况下的功能互操作情况。测试内容见 6.7.1.2 的规定。

6.10.4.3 行为互操作性测试

测试不同 IPsec 协议应用在 IKEv2 初始交换情况下的行为互操作情况。测试内容见 6.10.1.3 和 6.10.1.4 的规定。

6.11 IKEv2 创建子 SA 交换测试内容

6.11.1 功能测试内容

6.11.1.1 基本互连测试

测试在创建子 SA 交换情况下,IKEv2 协议的基本连通能力。

6.11.1.2 安全功能测试

测试在创建子 SA 交换情况下 IKEv2 协议支持的安全功能,测试内容包括:

a) 加密算法协商功能:能够支持 CHILD SA 中密码算法协商功能;
b) MAC 算法协商功能:能够支持 CHILD SA 中 MAC 算法协商功能;
c) 密钥协商功能:能够支持 CHILD SA 中共享密钥的协商功能;
d) 密钥更新功能:能够支持 IKE SA 和 CHILD SA 中密钥参数的刷新功能。

6.11.1.3 发起方行为测试

在创建子 SA 交换情况下,IKEv2 发起方行为测试内容如下:

a) 初始化时发起方接收到协商指示,构造 CREATE_CHILD_SA 请求消息并发送给响应方。CREATE_CHILD_SA 请求消息中包含安全关联载荷、密钥交换载荷,若要求实现密钥更新功能,则在消息中提供通知载荷。该消息格式应满足协议规范要求,并利用协商的算法和密钥进行加密。发起方提供该消息的超时重传功能,若重传次数超过指定的最大值,则终止本次协商。
b) 发起方接收 CREATE_CHILD_SA 响应消息。验证接收到的消息的合法性:若非法,则丢弃;否则,记录该消息中承载的协商结果,生成密钥并传递给 IPsec 安全协议。设置协商完成标志。
c) 发起方收到删除 CHILD SA 请求或收到 CHILD SA 到期通知,清除连接状态。

6.11.1.4 响应方行为测试

在创建子 SA 交换情况下,IKEv2 响应方行为测试内容如下:

a) 响应方等待接收 CREATE_CHILD_SA 请求消息。验证接收到的消息的合法性:若非法,则丢弃;否则,记录消息中承载的协商请求,根据本地情况确定安全关联的属性,构造 CREATE_CHILD_SA 响应消息并发送给发起方,生成密钥并传递给安全协议(如 AH 或 ESP)。该消息中包含安全关联载荷、密钥交换载荷,其格式应满足协议规范要求,利用协商的算法和密钥进行加密。
b) 响应方根据请求消息中的内容产生更新消息,将生成的密钥等信息传递给安全协议。
c) 响应方收到删除 CHILD SA 请求或收到 CHILD SA 到期通知,清除连接状态。

6.11.2 性能测试内容

测试在创建子 SA 交换情况下 IKEv2 协议的性能指标，测试内容包括：

a) 创建子 SA 交换时延：测量 IKEv2 协议建立 CHILD SA 的时延；
b) 单位时间新建子 SA 数：测量 IKEv2 协议每秒钟能够建立的 CHILD SA 连接数；
c) 设备支持的总连接数：测量 IKEv2 协议所能支持的 CHILD SA 连接总数；
d) 剩余错误比率：测量 IKEv2 协议协商报文的剩余错误比率；
e) 失败概率：测量 IKEv2 协议协商失败的概率，包括连接建立失败概率、传送失败概率等；
f) 密钥更新：测量 IKEv2 协议的密钥自动更新机制，如要求 IKE SA 的密钥更新周期不大于 24 h，CHILD SA 的密钥更新周期不大于 1 h。

6.11.3 健壮性测试内容

6.11.3.1 无效报文处理能力

测试在创建子 SA 交换情况下 IKEv2 协议的无效报文处理能力。测试内容见 6.7.3.1 的规定。

6.11.3.2 异常事件处理能力

测试在创建子 SA 交换情况下 IKEv2 协议的异常事件处理能力。测试内容见 6.7.3.2 的规定。

6.11.3.3 高强度负载处理能力

测试在创建子 SA 交换情况下 IKEv2 协议的高强度负载处理能力。测试内容见 6.7.3.3 的规定。

6.11.4 互操作性测试内容

6.11.4.1 基本互连测试

测试不同 IPsec 协议应用在创建子 SA 交换情况下的基本连通能力。

6.11.4.2 功能互操作性测试

测试不同 IPsec 协议应用在创建子 SA 交换情况下的功能互操作情况。测试内容见 6.11.1.2 的规定。

6.11.4.3 行为互操作性测试

测试不同 IPsec 协议应用在创建子 SA 交换情况下的行为互操作情况。测试内容见 6.11.1.3 和 6.11.1.4 的规定。

6.12 IKEv2 信息交换测试内容

6.12.1 功能测试内容

6.12.1.1 基本互连测试

测试在信息交换情况下，IKEv2 协议的基本连通能力。

6.12.1.2 安全功能测试

测试在信息交换情况下 IKEv2 协议支持的安全功能，测试内容包括：

a) 事件通知：能够传递交换过程中产生的事件；

b） 删除安全关联：能够协商删除指定的安全关联；
c） 配置参数：能够协商配置相关参数；
d） 活性探测：能够探测协商参与方的存活性。

6.12.2 性能测试内容

测试在信息交换情况下 IKEv2 协议的性能指标，测试内容包括：
a） 剩余错误比率：测量 IKEv2 协议报文的剩余错误比率；
b） 失败概率：测量 IKEv2 协议报文的传送失败概率。

6.12.3 健壮性测试内容

6.12.3.1 错误报文处理能力

测试接收到的 IKEv2 信息交换报文中有错误时，IKEv2 协议的处理能力。

6.12.3.2 异常事件处理能力

测试在信息交换情况下 IKEv2 协议的异常事件处理能力。测试内容见 6.7.3.2 的规定。

6.12.3.3 高强度负载处理能力

测试在信息交换情况下 IKEv2 协议的高强度负载处理能力。测试内容见 6.7.3.3 的规定。

6.12.4 互操作性测试内容

6.12.4.1 基本互连测试

测试不同 IPsec 协议应用在 IKEv2 信息交换情况下的基本连通能力。

6.12.4.2 功能互操作性测试

测试不同 IPsec 协议应用在 IKEv2 信息交换情况下的功能互操作情况。测试内容见 6.12.1.2 的规定。

7 测试步骤

7.1 AH 传输模式测试步骤

7.1.1 功能测试

7.1.1.1 基本互连测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下。
第二步：检查网络的物理连接情况。
第三步：检查网络的逻辑连通情况（如利用 ICMP 回送请求和回送响应测试）。
第四步：若上述检查未通过，则基本互连测试失败。

7.1.1.2 安全功能测试

测试 IPsec 协议应用在 AH 传输模式下的安全功能，测试步骤如下：
a） AH 传输模式功能测试
第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），等待被测设备的响应。

第三步：若收到 AH 传输模式封装的响应报文（如 ICMP 回送响应），则说明被测设备支持 AH 传输模式功能。

b） 数据完整性保护功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），等待被测设备的响应。

第三步：若收到 AH 传输模式封装的响应报文（如 ICMP 回送响应），且 AH 完整性校验值校验正确，则说明被测设备支持 AH 数据完整性保护功能。

c） 数据源认证功能测试

测试步骤同 7.1.1.2b）。

d） 抗重放攻击服务功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备发送序列号低于被测设备 AH SA 抗重放窗口左侧的 AH 传输模式报文（如 ICMP 回送请求）。

第三步：被测设备应该丢弃该 AH 报文，测试设备不应收到 AH 传输模式封装的响应报文（如 ICMP 回送响应）。

e） 应用 IPsec 策略功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，同时设置 SPD 策略为应用 IPsec，触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），等待返回的响应。

第三步：若测试设备收到 AH 传输模式封装的响应报文（如 ICMP 回送响应），且 AH 完整性校验值校验正确，则被测设备支持应用 IPsec 策略功能。

f） 旁路策略功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，同时设置 SPD 策略为旁路 IPsec，触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备发送未经过 AH 传输模式封装的请求报文（如 ICMP 回送请求），该报文符合旁路策略，等待返回的响应。

第三步：若测试设备收到未经过 AH 传输模式封装的响应报文（如 ICMP 回送响应），则被测设备支持旁路 IPsec 策略功能。

g） 丢弃策略功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，同时设置 SPD 策略为丢弃报文，触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备发送请求报文（如 ICMP 回送请求），该报文符合丢弃策略。

第三步：测试设备不应收到被测设备发送过来的响应报文（如 ICMP 回送响应）；否则，说明被测设备不支持丢弃策略功能。

h） SPD 策略选择功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，同时设置不同的安全策略（如分别利用地址、端口作为选择符），触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），等待返回的响应。

第三步：验证是否收到被测设备发送过来的 AH 传输模式封装的响应报文（如 ICMP 回送响应），且 AH 完整性校验值校验正确。

第四步：测试设备的某个端口向被测设备发送请求报文，等待返回的响应。

第五步：验证测试设备的另一个端口是否收到被测设备发送的 AH 传输模式封装的响应报文。

第六步：根据第三步和第五步的测试结果确定是否支持 SPD 策略选择功能。

i) SA 生存期功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下。

第二步：配置 SA 的生存期为 10 s，触发 IKE 进行 AH SA 协商。

第三步：测试设备向被测设备连续发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），得到被测设备返回的 AH 传输模式封装的响应报文（如 ICMP 回送响应）。

第四步：等待 10 s 后，测试设备向被测设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），检查是否能得到被测设备返回的响应报文。若不能，则被测设备支持 SA 生存期检测功能。

第五步：配置 SA 的生存期为 1KB，触发 IKE 重新进行 AH SA 协商。

第六步：测试设备向被测设备连续发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），检测是否可得到被测设备返回的 AH 传输模式封装的响应报文（如 ICMP 回送响应）。

第七步：当 ICMP 回送请求报文流量小于 1KB 时，可得到被测设备返回的 AH 传输模式封装的响应报文（如 ICMP 回送响应）。当 ICMP 回送请求报文流量大于 1KB 时，不能得到被测设备返回的响应报文。

第八步：根据第四步和第七步的测试结果确定被测设备是否支持 SA 生存期检测功能。

j) 分片重组功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备发送 AH 传输模式封装的请求报文（如 ICMP 回送请求），且该请求报文长度超过被测设备的 MTU。等待返回的响应报文。

第三步：若测试设备接收到响应报文（如 ICMP 回送请求），则被测设备支持分片重组功能。

k) 序号增长功能测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备向被测设备连续发送两个请求报文（如 ICMP 回送请求），等待返回的响应报文。

第三步：若响应报文（如 ICMP 回送请求）中的 AH 头部序号顺序增长，说明被测设备支持序号增长功能。

7.1.2 性能测试

测试 IPsec 协议应用在 AH 传输模式下的性能指标，测试步骤如下：

a) 吞吐量测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：创建不同长度的 AH 传输模式封装的数据包，构造以太网帧并发送。

第三步：记录所传送报文的总字节数和传输时间，计算获得吞吐量。

b) 传送时延测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：创建 AH 传输模式封装的数据包，构造以太网帧并发送。

第三步：记录所传送报文的长度、发送开始时间、接收响应的时间，计算传送时延。

c) 剩余错误比率测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：在一段时间内批量传输 AH 传输模式封装的数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：计算在此时间段内的剩余错误比率。

d) 失败概率测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：批量传输 AH 传输模式封装的数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：统计在此过程中的传送失败的概率。

7.1.3 健壮性测试

7.1.3.1 无效报文处理能力测试

测试 IPsec 协议应用在 AH 传输模式下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备构造错误报文并发送给被测设备。错误报文类型见 6.1.3.1a)。

第三步：被测设备应该丢弃该报文，根据配置情况可记录日志。

b) 非期望报文处理能力测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备构造非期望报文并发送给被测设备。非期望报文类型见 6.1.3.1b)。

第三步：被测设备应该丢弃该报文，根据配置情况可记录日志。

7.1.3.2 异常事件处理能力测试

测试 IPsec 协议应用在 AH 传输模式下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：断开物理连接。

第三步：测试设备发送 AH 传输模式封装的请求报文(如 ICMP 回送请求)给被测设备，并等待响应。测试设备不能接收到被测设备返回的响应报文(如 ICMP 回送响应)。

b) 无效 SA 处理能力测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：测试设备发送 AH 传输模式封装的请求报文(如 ICMP 回送请求)，等待被测设备的响应。

第三步：若收到被测设备返回的响应(如 ICMP 回送响应)且验证正确，则测试设备发送不同 SPI 值的报文，观察是否能够得到被测设备的响应。

第四步：被测设备丢弃该报文，测试设备不能收到返回的响应。

7.1.3.3 高强度负载处理能力测试

测试 IPsec 协议应用在 AH 传输模式下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：配置测试设备和被测设备均工作在 AH 传输模式下，触发 IKE 进行 AH SA 协商。

第二步：在网络负载很大（带宽占用率为90%以上）的情况下，发送AH传输模式封装的用户数据。

第三步：查看被测设备的处理能力。

b） 系统高强度负载处理能力测试

第一步：配置测试设备和被测设备均工作在AH传输模式下，触发IKE进行AH SA协商。

第二步：在被测设备高强度负载（内存、CPU占用率为90%以上）的情况下，发送AH传输模式封装的用户数据。

第三步：查看被测设备的处理能力。

7.1.4 互操作性测试

7.1.4.1 基本互连测试

设置不同IPsec协议应用均工作在AH传输模式下，进行基本互连测试。测试步骤见7.1.1.1。

7.1.4.2 功能互操作性测试

设置不同IPsec协议应用均工作在AH传输模式下，进行功能互操作性测试。测试步骤见7.1.1.2的规定。

7.2 AH隧道模式测试步骤

7.2.1 功能测试

7.2.1.1 基本互连测试

配置测试设备和被测设备均工作在AH隧道模式下，进行基本互连测试。测试步骤见7.1.1.1。

7.2.1.2 安全功能测试

配置测试设备和被测设备均工作在AH隧道模式下，进行安全功能测试。测试步骤见7.1.1.2的规定。

7.2.2 性能测试

配置测试设备和被测设备均工作在AH隧道模式下，进行性能测试。测试步骤见7.1.2的规定。

7.2.3 健壮性测试

7.2.3.1 无效报文处理能力测试

配置测试设备和被测设备均工作在AH隧道模式下，进行无效报文处理能力测试。测试步骤见7.1.3.1的规定。

7.2.3.2 异常事件处理能力测试

配置测试设备和被测设备均工作在AH隧道模式下，进行异常事件处理能力测试。测试步骤见7.1.3.2的规定。

7.2.3.3 高强度负载处理能力测试

配置测试设备和被测设备均工作在AH隧道模式下，进行高强度负载处理能力测试。测试步骤见7.1.3.3的规定。

7.2.4 互操作性测试

7.2.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 AH 隧道模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.2.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 AH 隧道模式下，进行功能互操作性测试。测试步骤见 7.1.1.2 的规定。

7.3 ESP 传输模式测试步骤

7.3.1 功能测试

7.3.1.1 基本互连测试

配置测试设备和被测设备均工作在 ESP 传输模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.3.1.2 安全功能测试

测试 IPsec 协议应用在 ESP 传输模式下的安全功能，测试步骤如下：

a) ESP 传输模式功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送 ESP 传输模式封装的请求报文（如 ICMP 回送请求），等待被测设备的响应。

第三步：若收到 ESP 传输模式封装的响应报文（如 ICMP 回送响应），则说明被测设备支持 ESP 传输模式功能。

b) 数据完整性保护功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送 ESP 传输模式封装的请求报文（如 ICMP 回送请求），等待被测设备的响应。

第三步：若收到 ESP 传输模式封装的响应报文（如 ICMP 回送响应），包含 ESP 认证数据，且 ESP 完整性校验值校验正确，则说明支持 ESP 数据完整性保护功能。

c) 数据源认证功能测试

测试步骤同 7.3.1.2b）。

d) 数据保密性功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送 ESP 传输模式封装的请求报文（如 ICMP 回送请求），等待被测设备的响应。

第三步：若收到 ESP 传输模式封装的响应报文（如 ICMP 回送响应），且 ESP 封装内容解密正确，则说明支持 ESP 数据保密性保护功能。

e) 抗重放攻击服务功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送序列号低于被测设备 ESP SA 抗重放窗口左侧的 ESP 传输模式报文（如 ICMP 回送请求）。

第三步：被测设备应该丢弃该 ESP 报文，测试设备不能收到 ESP 传输模式封装的响应报文（如

ICMP 回送响应)。

f) 应用 IPsec 策略功能测试

第一步:配置测试设备和被测设备均工作在 ESP 传输模式下,同时设置 SPD 策略为应用 IPsec,触发 IKE 进行 ESP SA 协商。

第二步:测试设备向被测设备发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求),等待返回的响应。

第三步:验证是否收到 ESP 传输模式封装的响应报文(如 ICMP 回送响应),且 ESP 解密及完整性校验值校验正确。若是,则被测设备支持应用 IPsec 策略功能。

g) 旁路策略功能测试

第一步:配置测试设备和被测设备均工作在 ESP 传输模式下,同时设置 SPD 策略为旁路 IPsec,触发 IKE 进行 ESP SA 协商。

第二步:测试设备向被测设备发送未经过 ESP 传输模式封装的请求报文(如 ICMP 回送请求),该报文符合旁路策略,等待返回的响应。

第三步:若测试设备收到未经过 ESP 传输模式封装的响应报文(如 ICMP 回送响应),则被测设备支持旁路 IPsec 策略功能。

h) 丢弃策略功能测试

第一步:配置测试设备和被测设备均工作在 ESP 传输模式下,同时设置 SPD 策略为丢弃报文,触发 IKE 进行 ESP SA 协商。

第二步:测试设备向被测设备发送请求报文(如 ICMP 回送请求),该报文符合丢弃策略。

第三步:测试设备不应收到被测设备发送过来的响应报文(如 ICMP 回送响应);否则,说明被测设备不支持丢弃策略功能。

i) SPD 策略选择功能测试

第一步:配置测试设备和被测设备均工作在 ESP 传输模式下,并设置不同的安全策略(如分别利用地址、端口作为选择符),触发 IKE 进行 ESP SA 协商。

第二步:测试设备向被测设备发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求),等待返回的响应。

第三步:验证测试设备是否收到被测设备发送过来的 ESP 传输模式封装的响应报文(如 ICMP 回送响应),且 ESP 解密及完整性校验值校验正确。

第四步:测试设备的某个端口向被测设备发送请求报文,等待返回的响应。

第五步:测试设备的另一个端口是否收到被测设备发送的 ESP 传输模式封装的响应报文。

第六步:根据第三步和第五步的测试结果确定是否支持 SPD 策略选择功能。

j) SA 生存期功能测试

第一步:配置测试设备和被测设备均工作在 ESP 传输模式下。

第二步:配置 SA 的生存期为 10 s,触发 IKE 进行 ESP SA 协商。

第三步:测试设备向被测设备连续发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求),可得到被测设备返回的 ESP 传输模式封装的响应报文(如 ICMP 回送响应)。

第四步:等待 10 s 后,测试设备发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求),检查是否能得到被测设备返回响应报文。若不能,则被测设备支持 SA 生存期检测功能。

第五步:配置 SA 的生存期为 1 KB,触发 IKE 重新进行 ESP SA 协商。

第六步:测试设备向被测设备连续发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求),检测是否可得到返回的 ESP 传输模式封装的响应报文(如 ICMP 回送响应)。

第七步:当 ICMP 回送请求报文流量小于 1 KB 时,可得到被测设备返回的 ESP 传输模式封装的响应报文(如 ICMP 回送响应)。当 ICMP 回送请求报文流量大于 1 KB 时,不能得到被测

设备返回的响应报文。

第八步：根据第四步和第七步的测试结果确定被测设备是否支持 SA 生存期检测功能。

k） 分片重组功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备向被测设备发送 ESP 传输模式封装请求报文（如 ICMP 回送请求），且该请求报文长度超过被测设备的 MTU。等待返回的响应报文。

第三步：若测试设备接收到响应报文（如 ICMP 回送请求），则被测设备支持分片重组功能。

l） 序号增长功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备向被测设备连续发送两个请求报文（如 ICMP 回送请求），等待返回的响应报文。

第三步：若响应报文（如 ICMP 回送请求）中的 ESP 头部序号顺序增长，说明被测设备支持序号增长功能。

m） NAT 穿越功能测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，被测设备位于 NAT 后，触发 IKE 进行 ESP SA 协商。

第二步：由被测设备向测试设备发送请求报文（如 ICMP 回送请求），等待返回的响应报文。

第三步：测试设备检查收到报文，处理方法如下：

1） 检查 UDP 封装的报文中源端口或目的端口是否更新（如更新为 4500），若不是，则直接返回；

2） 检查 UDP 头部后的四个字节是否为 0，若为 0，则直接返回；

3） 进行 UDP 传输模式封装的 ESP 头部的解封装处理，还原生成原始的 ESP 报文，检测是否为被测设备发送的请求报文，若不是则返回；

4） 构造响应报文（如 ICMP 回送请求）并返回，同样响应报文需要在 ESP 加密之后进行 UDP 封装处理。

第四步：若测试设备检测到 UDP 传输模式封装的 ESP 报文且能与被测设备能正常通信，则说明被测设备支持 NAT 穿越功能。

7.3.2 性能测试

测试 IPsec 协议应用在 ESP 传输模式下的性能指标，测试步骤如下：

a） 加解密吞吐量测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：创建不同长度的 ESP 传输模式封装的数据包，构造以太网帧并发送。

第三步：记录被测设备内部接口上所收发报文的总字节数和传输时间，计算获得吞吐量。

b） 加解密时延测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：创建不同长度的 ESP 传输模式封装的数据包，构造以太网帧并发送。

第三步：记录所传送报文的总字节数、发送时间及接收到响应的时间等，统计计算加解密时延。

c） 传送时延测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：创建 ESP 传输模式封装的数据包，构造以太网帧并发送，等待返回的响应。

第三步：记录所传送报文的长度、发送开始时间、接收响应的时间，计算传送时延。

d） 剩余错误比率测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：在某段时间内批量传输数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：计算在此时间段内的剩余错误比率。

e) 失败概率测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：批量传输数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：统计在此过程中的传送失败的概率。

7.3.3 健壮性测试

7.3.3.1 无效报文处理能力测试

测试 IPsec 协议应用在 ESP 传输模式下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备构造错误报文并发送给被测设备。错误报文类型见 6.3.3.1a)。

第三步：被测设备应该丢弃该报文，根据配置情况可记录日志。

b) 非期望报文处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备构造非期望报文并发送给被测设备。非期望报文类型见 6.3.3.1b)。

第三步：被测设备应该丢弃该报文，根据配置情况可记录日志。

7.3.3.2 异常事件处理能力测试

测试 IPsec 协议应用在 ESP 传输模式下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：断开物理网络连接。

第三步：测试设备发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求)给被测设备，并等待响应。测试设备不能接收到被测设备返回的响应报文(如 ICMP 回送响应)。

b) 无效 SA 处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送 ESP 传输模式封装的请求报文(如 ICMP 回送请求)，等待被测设备的响应。

第三步：若收到被测设备返回的响应(如 ICMP 回送响应)且验证正确，则测试设备发送不同 SPI 值的报文，观察是否能够得到被测设备的响应。

第四步：被测设备丢弃该报文，测试设备不能收到返回的响应。

7.3.3.3 高强度负载处理能力测试

测试 IPsec 协议应用在 ESP 传输模式下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：在网络负载很大(带宽占用率为 90%以上)的情况下，发送 ESP 传输模式封装的用户

数据。

第三步：查看被测设备的处理能力。

b） 系统高强度负载处理能力测试

第一步：配置测试设备和被测设备均工作在 ESP 传输模式下，触发 IKE 进行 ESP SA 协商。

第二步：在被测设备高强度负载（内存、CPU 占用率为 90%以上）的情况下，发送 ESP 传输模式封装的用户数据。

第三步：查看被测设备的处理能力。

7.3.4 互操作性测试

7.3.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 ESP 传输模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.3.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 ESP 传输模式下，进行功能互操作性测试。测试步骤见7.3.1.2的规定。

7.4 ESP 隧道模式测试步骤

7.4.1 功能测试

7.4.1.1 基本互连测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.4.1.2 安全功能测试

测试 IPsec 协议应用在 ESP 隧道模式下的安全功能，测试步骤如下：

a） 基本安全功能测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行基本安全功能测试。测试步骤见7.3.1.2的规定。

b） 有限业务流的保密性保护功能测试

第一步：配置测试设备和被测设备均工作在 ESP 隧道模式下，触发 IKE 进行 ESP SA 协商。

第二步：测试设备发送 ESP 隧道模式封装的请求报文（如 ICMP 回送请求），等待返回的响应。

第三步：若收到 ESP 隧道模式封装的响应报文（如 ICMP 回送响应），ESP 封装内容解密正确且提供了填充数据隐藏内部报文，则支持 ESP 有限业务流的保密性保护功能。

7.4.2 性能测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行性能测试。测试步骤见 7.3.2 的规定。

7.4.3 健壮性测试

7.4.3.1 无效报文处理能力测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行无效报文处理能力测试。测试步骤见7.3.3.1的规定。

7.4.3.2 异常事件处理能力测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行异常事件处理能力测试。测试步骤见

7.3.3.2的规定。

7.4.3.3 高强度负载处理能力测试

配置测试设备和被测设备均工作在 ESP 隧道模式下，进行高强度负载处理能力测试。测试步骤见7.3.3.3 的规定。

7.4.4 互操作性测试

7.4.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 ESP 隧道模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.4.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 ESP 隧道模式下，进行功能互操作性测试。测试步骤见7.4.1.2的规定。

7.5 传输邻接模式测试步骤

7.5.1 功能测试

7.5.1.1 基本互连测试

配置测试设备和被测设备均工作在传输邻接模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.5.1.2 安全功能测试

测试 IPsec 协议应用在传输邻接模式下的安全功能，测试步骤如下：

a) 传输邻接模式功能测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 的协商。

第二步：测试设备发送传输邻接模式封装的请求报文(如 ICMP 回送请求)，等待返回的响应。

第三步：若收到传输邻接模式封装的响应报文(如 ICMP 回送响应)，则说明被测设备支持传输邻接模式功能。

b) 数据完整性保护功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行数据完整性保护功能测试。测试步骤见 7.1.1.2b)。

c) 数据源认证功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行数据源认证功能测试。测试步骤见7.1.1.2c)。

d) 数据保密性功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行数据保密性功能测试。测试步骤见7.3.1.2d)。

e) 抗重放攻击服务功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行抗重放攻击服务功能测试。测试步骤见 7.1.1.2d)。

f) 应用 IPsec 策略功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行应用 IPsec 策略功能测试。测试步骤见 7.1.1.2e)。

g) 旁路策略功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行旁路 IPsec 策略功能测试。测试步骤见 7.1.1.2f)。

h) 丢弃策略功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行丢弃策略功能测试。测试步骤见 7.1.1.2g)。

i) SPD 策略选择功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行 SPD 策略选择功能测试。测试步骤见 7.1.1.2h)。

j) SA 生存期功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行 SA 生存期功能测试。测试步骤见 7.1.1.2i)。

k) 分片重组功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行分片重组功能测试。测试步骤见 7.1.1.2j)。

l) 序号增长功能测试

配置测试设备和被测设备均工作在传输邻接模式下，进行序号增长功能测试。测试步骤见 7.1.1.2k)。

7.5.2 性能测试

测试 IPsec 协议应用在传输邻接模式下的性能指标，测试步骤如下：

a) 加解密吞吐量测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 协商。

第二步：创建不同长度的传输邻接模式封装的数据包，构造以太网帧并发送。

第三步：记录被测设备内部接口上所收发报文的总字节数和传输时间，计算获得吞吐量。

b) 加解密时延测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 协商。

第二步：创建不同长度的传输邻接模式封装的数据包，构造以太网帧并发送。

第三步：记录所传送报文的总字节数、发送时间及接收到响应的时间等，统计计算加解密时延。

c) 传送时延测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 协商。

第二步：创建传输邻接模式封装的数据包，构造以太网帧并发送，等待返回的响应。

第三步：记录所传送报文的长度、发送开始时间、接收响应的时间，计算传送时延。

d) 剩余错误比率测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 协商。

第二步：在某段时间内批量传输数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：计算在此时间段内的剩余错误比率。

e) 失败概率测试

第一步：配置测试设备和被测设备均工作在传输邻接模式下，触发 IKE 进行 SA 协商。

第二步：批量传输数据，记录所传送报文个数、总字节数、传输失败的报文个数、传输失败的字节数。

第三步：统计在此过程中的传送失败的概率。

7.5.3 健壮性测试

7.5.3.1 无效报文处理能力测试

测试 IPsec 协议应用在传输邻接模式下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行错误报文处理能力测试。错误报文类型见 6.5.3.1a)，测试步骤见 7.1.3.1a)。

b) 非期望报文处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行错误报文处理能力测试。非期望报文类型见 6.5.3.1b)，测试步骤见 7.1.3.1b)。

7.5.3.2 异常事件处理能力测试

测试 IPsec 协议应用在传输邻接模式下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行连接中断处理能力测试。测试步骤见 7.1.3.2a)。

b) 无效 SA 处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行无效 SA 处理能力测试。测试步骤见 7.1.3.2b)。

7.5.3.3 高强度负载处理能力测试

测试 IPsec 协议应用在传输邻接模式下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行网络高强度负载处理能力测试。测试步骤见 7.1.3.3a)。

b) 系统高强度负载处理能力测试

配置测试设备和被测设备均工作在传输邻接模式下，进行系统高强度负载处理能力测试。测试步骤见 7.1.3.3b)。

7.5.4 互操作性测试

7.5.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在传输邻接模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.5.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在传输邻接模式下，进行功能互操作性测试。测试步骤见 7.5.1.2 的规定。

7.6 迭代隧道模式测试步骤

7.6.1 功能测试

7.6.1.1 基本互连测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行基本互连测试。测试步骤见 7.1.1.1。

7.6.1.2 安全功能测试

测试 IPsec 协议应用在迭代隧道模式下的安全功能，测试步骤如下：

a) 迭代隧道模式功能测试

第一步：配置测试设备和被测设备均工作在迭代隧道模式下，触发 IKE 进行 SA 的协商。

第二步：测试设备发送迭代隧道模式封装的请求报文(如 ICMP 回送请求)，等待返回的响应。

第三步：若收到迭代隧道模式封装的响应报文(如 ICMP 回送响应)，则说明被测设备支持迭代隧道模式功能。

b) 数据完整性保护功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行数据完整性保护功能测试。测试步骤见 7.1.1.2b)。

c) 数据源认证功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行数据源认证功能测试。测试步骤见 7.1.1.2c)。

d) 数据保密性功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行数据保密性功能测试，测试步骤同 7.3.1.2d)。

e) 有限业务流的保密性保护功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行有限业务流的保密性保护功能测试，测试步骤见 7.4.1.2b)。

f) 抗重放攻击服务功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行抗重放攻击服务功能测试。测试步骤见 7.1.1.2d)。

g) 应用 IPsec 策略功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行应用 IPsec 策略功能测试。测试步骤见 7.1.1.2e)。

h) 旁路策略功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行旁路策略功能测试。测试步骤见 7.1.1.2f)。

i) 丢弃策略功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行丢弃策略功能测试。测试步骤见 7.1.1.2g)。

j) SPD 策略选择功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行 SPD 策略选择功能测试。测试步骤见 7.1.1.2h)。

k) SA 生存期功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行 SA 生存期功能测试。测试步骤见 7.1.1.2i)。

l) 分片重组功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行分片重组功能测试。测试步骤见 7.1.1.2j)。

m) 序号增长功能测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行序号增长功能测试。测试步骤见

7.1.1.2k)。

7.6.2 性能测试

测试 IPsec 协议应用在迭代隧道模式下的性能指标，测试步骤见 7.3.2 的规定。

7.6.3 健壮性测试

7.6.3.1 无效报文处理能力测试

测试 IPsec 协议应用在迭代隧道模式下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行错误报文处理能力测试。错误报文类型见 6.5.3.1a)，测试步骤见 7.1.3.1a)。

b) 非期望报文处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行非期望报文处理能力测试。非期望报文类型见 6.5.3.1b)，测试步骤见 7.1.3.1b)。

7.6.3.2 异常事件处理能力测试

测试 IPsec 协议应用在迭代隧道模式下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行连接中断处理能力测试。测试步骤见 7.1.3.2a)。

b) 无效 SA 处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行无效 SA 处理能力测试。测试步骤见 7.1.3.2b)。

7.6.3.3 高强度负载处理能力测试

测试 IPsec 协议应用在迭代隧道模式下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行网络高强度负载处理能力测试。测试步骤见 7.1.3.3a)。

b) 系统高强度负载处理能力测试

配置测试设备和被测设备均工作在迭代隧道模式下，进行系统高强度负载处理能力测试。测试步骤见 7.1.3.3b)。

7.6.4 互操作性测试

7.6.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在迭代隧道模式下，实现基本互连测试。测试步骤见 7.1.1.1。

7.6.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在迭代隧道模式下，实现功能互操作性测试。测试步骤见 7.6.1.2 的规定。

7.7 IKEv1 主模式测试步骤

7.7.1 功能测试

7.7.1.1 基本互连测试

第一步：配置 IPsec 协议应用工作在 IKEv1 主模式交换情况下。
第二步：检查网络的物理连接情况。
第三步：检查网络的逻辑连通情况（如利用 ICMP 回送请求和回送响应测试）。
第四步：触发 IKE 进行 SA 的协商，检查是否能传递 IKE 报文。
第五步：若上述检查未通过，则基本互连测试失败。

7.7.1.2 安全功能测试

测试 IKEv1 协议在主模式交换情况下的安全功能，测试步骤如下：

a) 身份认证方法协商功能测试
第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。
第二步：查看消息 1 中的 SA 属性载荷部分。若没有认证方式的属性载荷，则不支持身份认证方法的协商功能。
第三步：查看消息 2 中的 SA 属性载荷部分。若没有认证方式的属性载荷，则不支持身份认证方法的协商功能。

b) 身份认证协商过程测试
第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。
第二步：解密消息 5，检查消息体中的认证部分（如 HASH 载荷或 SIG 载荷），根据协商的步骤、算法和密钥验证其正确性：若不正确，则身份认证协商失败。
第三步：解密消息 6，检查消息体中的认证部分（如 HASH 载荷或 SIG 载荷），根据协商的步骤、算法和密钥验证其正确性：若不正确，则身份认证协商失败。

c) 加密算法协商功能测试
第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。
第二步：查看消息 1 中是否有加密属性载荷。若有，则发起方支持加密算法协商功能。
第三步：查看消息 2 中是否有加密属性载荷。若有，则响应方支持加密算法协商功能。
第四步：查看协商好的 ISAKMP SA 中是否有数据加密算法。若有，则说明支持加密算法协商功能。

d) 伪随机函数 PRF 协商功能
第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。
第二步：查看消息 1 中是否有伪随机函数 PRF 的属性载荷。若有，则发起方支持伪随机函数 PRF 协商功能。
第三步：查看消息 2 中是否有伪随机函数 PRF 的属性载荷。若有，则响应方支持伪随机函数 PRF 协商功能。
第四步：查看协商好的 ISAKMP SA 中是否有伪随机函数 PRF。若有，则说明支持伪随机函数 PRF 协商功能。

e) 密钥协商功能测试
第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。
第二步：查看消息 3 中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。
第三步：查看消息 4 中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第四步：查看协商好的 ISAKMP SA 中密钥是否存在。若存在，则说明支持密钥协商功能。

f) 数据加密功能测试

第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。

第二步：查看消息 5 中的 ISAKMP 头部的加密比特标志位是否设置，若设置，则使用协商好的算法和密钥进行解密。若解密正确，则支持数据加密功能。

第三步：查看消息 6 中的 ISAKMP 头部的加密比特标志位是否设置。若设置，则使用协商好的算法和密钥进行数据解密，以此验证数据加密功能。

g) NAT 穿越探测功能

第一步：配置 IPsec 协议应用，在连接中设置 NAT 设备，触发 IKEv1 主模式交换。

第二步：查看消息 1 中是否有 VID 载荷。若有，检测其值是否符合标准值。若是，则发起方支持 NAT 穿越功能。

第三步：查看消息 2 中是否有 VID 载荷。若有，检测其值是否符合标准值。若是，则响应方支持 NAT 穿越功能。

第四步：查看消息 3 中是否有 NAT-D 载荷。若有，则发起方支持 NAT 穿越探测功能。

第五步：查看消息 4 中是否有 NAT-D 载荷。若有，则响应方支持 NAT 穿越探测功能。

第六步：查看消息 5 中的 UDP 头部中端口是否更新(如更新为 4500)。若是，则发起方支持 NAT 穿越 UDP 封装功能。

第七步：查看消息 6 中的 UDP 头部中端口是否更新(如更新为 4500)。若是，则响应方支持 NAT 穿越 UDP 封装功能。

第八步：若 IPsec 协议应用的上述检查通过，则支持 NAT 穿越探测功能。

h) NAT KEEPALIVE 功能

第一步：配置 IPsec 协议应用，在连接中设置 NAT 设备，触发 IKEv1 主模式交换。

第二步：检查是否收到 NAT KEEPALIVE 报文。若是，则支持 NAT KEEPALIVE 功能。

7.7.1.3 发起方行为测试

测试 IKEv1 协议在主模式交换情况下发起方的行为(其行为状态参见附录 B.2.1.5)，测试步骤如下：

a) START 状态测试

第一步：配置参数，触发发起方 IPsec 协议(如 AH 或 ESP)产生连接请求。

第二步：查看接收到的消息是否为消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 1 结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

b) MAIN_I1 状态测试

MAIN_I1 状态测试步骤如下：

1) 正常情况

第一步：发送消息 2，查看发起方的行为。

第二步：查看接收到的消息是否为消息 3。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 3 包含的载荷类型是否正确(与认证方式有关)，该消息结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

2) 非期望消息处理

第一步：向发起方发送消息 2 以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 2。

第二步：发起方应超时重传消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 2 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号、响应方 Cookie 设置为 0，建议和变换载荷包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 2 中包含非法的载荷类型。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 2，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv1 协议规范要求。

c） MAIN_I2 状态测试

MAIN_I2 状态测试步骤如下：

1） 正常情况

第一步：发送消息 4，查看发起方的行为。

第二步：查看接收到的消息是否为消息 5。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：验证消息 5 解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看消息 5 中载荷类型是否正确（与认证方式有关），该消息结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

第五步：验证消息 5 中的签名、HASH 值是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：发送消息 4 以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 4。

第二步：发起方应超时重传消息 3。若不是，则发起方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 4 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号，载荷包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 4 中包含非法载荷类型。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 4，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv1 协议规范要求。

d) MAIN_I3 状态测试

MAIN_I3 状态测试步骤如下：

1) 正常情况

第一步：发送消息 6，查看发起方的行为。

第二步：发起方进入连接状态，协商完成。

2) 非期望消息

第一步：向发起方发送消息 6 以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

3) 延迟发送

第一步：延迟发送消息 6。

第二步：发起方应超时重传消息 5。若不是，则发起方行为不符合 IKEv1 协议规范要求。

4) 提供非法参数

第一步：在消息 6 中提供非法参数（如该消息头部 HDR 中设置不同于消息 1 的版本号、清除加密标志，载荷包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

5) 错误消息

第一步：在消息 6 中包含非法载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

6) 重传计数器超过最大值

第一步：延迟发送消息 6，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv1 协议规范要求。

e) MAIN_I4 状态测试

MAIN_I4 状态测试步骤如下：

1) 正常情况

第一步：设置连接状态，阶段 1 协商完成。

第二步：指示可以开始阶段 2 的协商。

2) SA 管理

第一步：ISAKMP SA 到期或接收到删除 ISAKMP SA 请求。

第二步：发起方应该清除连接状态，进入 CLOSED 状态。若不是，则发起方行为不符合 IKEv1 协议规范要求。

7.7.1.4 响应方行为测试

测试 IKEv1 协议在主模式交换情况下响应方的行为（其行为状态参见附录 B 的 B.2.1.6），测试步骤如下：

a) START 状态测试

START 状态测试步骤如下：

1) 正常情况

第一步：发送消息 1，查看响应方的行为。

第二步：查看接收到的消息是否为消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 2 中 SA 的建议和变换载荷是否正确，该消息结构是否合法。若不合法，则响应方行为不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：向响应方发送消息 1 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 提供非法参数

第一步：在消息 1 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号、标志位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 错误消息

第一步：在消息 1 中包含非法载荷类型。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

b） MAIN_R1 状态测试

MAIN_R1 状态测试步骤如下：

1） 正常情况

第一步：发送消息 3，查看响应方的行为。

第二步：查看接收到的消息是否为消息 4。若不是，则响应方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 4 中载荷是否正确（与认证方法有关），该消息结构是否合法。若不合法，则响应方不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：发送消息 3 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 3。

第二步：响应方应超时重传消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 3 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 3 中包含非法的载荷类型。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IPsec 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 3，直到响应方的重传计数器值超过指定的最大值。

第二步：响应方应该清除状态，终止协商。若不是，则响应方行为不符合 IKEv1 协议规范要求。

c） MAIN_R2 状态测试

MAIN_R2 状态测试步骤如下：

1） 正常情况

第一步：发送消息 5，查看响应方的行为。

第二步：查看接收到的消息是否为消息 6。若不是，则响应方不符合 IKEv1 协议规范要求。

第三步：验证消息 6 解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看消息 6 中载荷类型是否正确，该消息结构是否合法。若不合法，则响应方不符合 IKEv1 协议规范要求。

第五步：验证消息 6 中的签名、HASH 值是否正确。若不正确，则响应方行为不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：发送消息 5 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 5。

第二步：响应方应超时重传消息 4。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 5 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号、清除加密标志，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 5 中包含非法载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IPsec 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 5，直到响应方的重传计数器值超过指定的最大值。

第二步：响应方应该清除状态，终止协商。若不是，则响应方行为不符合 IKEv1 协议规范要求。

d） MAIN_R3 状态测试

MAIN_R3 状态测试步骤如下：

1） 正常情况处理能力测试

第一步：设置连接状态，阶段 1 协商完成。

第二步：指示可以开始阶段 2 的协商。

2） SA 管理

第一步：ISAKMP SA 到期或接收到删除 ISAKMP SA 请求。

第二步：响应方应该清除连接状态，进入 CLOSED 状态。若不是，则响应方行为不符合 IKEv1 协议规范要求。

7.7.2 性能测试

测试 IKEv1 在主模式交换情况下的性能指标，测试步骤如下：

a） 连接建立时延

第一步：配置 IPsec 协议应用，设置为支持的认证方式，触发 IKEv1 主模式交换。

第二步：统计主模式连接建立时延。

b） 单位时间新建连接数

第一步：配置 IPsec 协议应用，设置为支持的认证方式。

第二步：配置发起方产生多个连接请求，触发 IKEv1 主模式交换。

第三步：测试单位时间内成功建立的连接数。

c） 设备支持的总连接数

第一步：配置 IPsec 协议应用，设置为支持的认证方式，触发 IKEv1 主模式交换。

第二步：配置发起方持续产生连接请求，保持建立的连接不释放。

第三步：在响应方不能接受连接时统计已经成功建立的连接数。

d) 剩余错误比率

第一步：配置 IPsec 协议应用，设置 IKEv1 为支持的主模式认证方式，并多次建立连接，传送数据，然后关闭连接。

第二步：统计在此过程中传送不正确、丢失或者重复的数据量和有效的数据量之比。

e) 失败概率

第一步：配置 IPsec 协议应用，设置 IKEv1 为支持的主模式认证方式，并多次建立连接、传送数据，然后关闭连接。

第二步：统计在此过程中的连接建立失败概率和传送失败概率。

f) 密钥更新

第一步：配置 IPsec 协议应用，设置 ISAKMP SA 的更新周期(如 24 h)，触发 IKEv1 主模式交换，保持连接。

第二步：在指定时间间隔(如 24 h)后查看 ISAKMP SA 状态，是否已经重新协商并更新密钥。

第三步：若未更新密钥，则不支持密钥更新功能。

7.7.3 健壮性测试

7.7.3.1 无效报文处理能力测试

测试 IKEv1 协议在主模式交换情况下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

在主模式消息交换过程中发送错误报文，测试 IKEv1 协议的处理能力。测试步骤见 7.7.1.3 和 7.7.1.4 中各状态下提供非法参数测试步骤和错误消息测试步骤。

b) 非期望报文处理能力测试

在主模式消息交换过程中发送非期望消息，测试 IKEv1 协议的处理能力。测试步骤见 7.7.1.3 和 7.7.1.4 中各状态下非期望消息的测试步骤。

7.7.3.2 异常事件处理能力测试

测试 IKEv1 协议在主模式交换情况下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

第一步：配置 IPsec 协议应用，触发 IKEv1 主模式交换。

第二步：断开物理网络连接。

第三步：IKEv1 应该重传报文，直到达到最大重传计数值，终止协商。

b) 等待超时处理能力测试

在主模式消息交换过程中延长数据交互时间直到超时，测试 IKEv1 协议的处理能力。测试步骤见 7.7.1.3 和 7.7.1.4 中各状态下延迟发送测试步骤和重传计数器超过最大值的测试步骤。

7.7.3.3 高强度负载处理能力测试

测试 IKEv1 协议在主模式交换情况下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：在网络负载很大(带宽占用率为 90%以上)的情况下，触发 IKEv1 主模式交换过程。

第二步：查看 IKEv1 的处理能力。

b) 系统高强度负载处理能力测试

第一步：在系统高强度负载(内存、CPU 占用率为 90%以上)的情况下，触发 IKEv1 主模式交

换过程。

第二步：查看 IKEv1 的处理能力。

7.7.4 互操作性测试

7.7.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv1 主模式交换情况下，进行基本连通测试。测试步骤见7.7.1.1。

7.7.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 主模式交换情况下，进行功能互操作性测试。测试步骤见 7.7.1.2 的规定。

7.7.4.3 行为互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 主模式交换情况下，进行行为互操作性测试。测试步骤见 7.7.1.3 和 7.7.1.4 的规定。

7.8 IKEv1 野蛮模式测试步骤

7.8.1 功能测试

7.8.1.1 基本互连测试

配置 IPsec 协议应用工作在 IKEv1 阶段 1 的野蛮模式交换方式，进行基本互连测试。测试步骤见7.7.1.1。

7.8.1.2 安全功能测试

测试 IKEv1 协议在野蛮模式交换情况下的安全功能，测试步骤如下：

a) 身份认证方法协商功能测试

测试 IKEv1 协议在野蛮模式交换情况下的身份认证方法协商功能，测试步骤见 7.7.1.2a)。

b) 身份认证协商过程测试

第一步：配置 IPsec 协议应用，触发 IKEv1 野蛮模式交换。

第二步：检查消息 2 中的认证部分(如 HASH 载荷或 SIG 载荷)，根据协商的步骤、算法和密钥验证其正确性：若不正确，则身份认证协商失败。

第三步：检查消息 3 中的认证部分(如 HASH 载荷或 SIG 载荷)，根据协商的步骤、算法和密钥验证其正确性：若不正确，则身份认证协商失败。

c) 加密算法协商功能测试

测试 IKEv1 协议在野蛮模式交换情况下的加密算法协商功能，测试步骤见 7.7.1.2c)。

d) 伪随机函数 PRF 协商功能

测试 IKEv1 协议在野蛮模式交换情况下的伪随机函数 PRF 协商功能，测试步骤见 7.7.1.2d)。

e) 密钥协商功能测试

第一步：配置 IPsec 协议应用，触发 IKEv1 野蛮模式交换。

第二步：查看消息 1 中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第三步：查看消息 2 中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第四步：查看协商好的 ISAKMP SA 中密钥是否存在。若存在，则说明支持密钥协商功能。

f) NAT 穿越探测功能

第一步：配置 IPsec 协议应用，触发 IKEv1 野蛮模式交换。

第二步：查看消息 1 中是否有 VID 载荷。若有，检测其值是否符合标准值。若是，则发起方支持 NAT 穿越功能。

第三步：查看消息 2 中是否有 VID 载荷。若有，检测其值是否符合标准值。若是，则响应方支持 NAT 穿越功能。同时检测消息 2 中是否有 NAT-D 载荷。若有，则响应方支持 NAT 穿越探测功能。

第四步：查看消息 3 中是否有 NAT-D 载荷。若有，则发起方支持 NAT 穿越探测功能。查看消息 3 中的 UDP 头部中端口是否更新（如更新为 4500）。若是，则发起方支持 NAT 穿越 UDP 封装功能。

第五步：查看响应方传递过来的报文中的 UDP 头部中端口是否更新（如更新为 4500）。若是，则响应方支持 NAT 穿越 UDP 封装功能。

第六步：若 IPsec 协议应用的上述检查通过，则支持 NAT 穿越探测功能。

g) NAT KEEPALIVE 功能

测试 IKEv1 协议在野蛮模式交换情况下的 NAT KEEPALIVE 功能，测试步骤见7.7.1.2 h）。

7.8.1.3 发起方行为测试

测试 IKEv1 协议在野蛮模式交换情况下发起方的行为（其行为状态见附录 B 的 B.2.2.5），测试步骤如下：

a) START 状态测试

第一步：配置参数，触发发起方 IPsec 协议（如 AH 或 ESP）产生连接请求。

第二步：查看接收到的消息是否为消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 1 结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

b) AGGR_I1 状态测试

AGGR_I1 状态测试步骤如下：

1) 正常情况

第一步：发送消息 2，查看发起方的行为。

第二步：查看接收到的消息是否为消息 3。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 3 的结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

第四步：验证消息 3 中的签名、HASH 是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

2) 非期望消息

第一步：发送消息 2 以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

3) 延迟发送

第一步：延迟发送消息 2。

第二步：发起方应超时重传消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

4) 提供非法参数

第一步：在消息 2 中提供非法参数（如消息头部 HDR 中设置非法参数，如设置不同于消息 1 的版本号、响应方 Cookie 设置为 0，载荷包含不在协议规范中定义的值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 2 中包含非法的载荷类型。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 2，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv1 协议规范要求。

c） AGGR_I2 状态测试

AGGR_I2 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态，阶段 1 协商完成。

第二步：指示可以开始阶段 2 的协商。

2） SA 管理

第一步：ISAKMP SA 到期或接收到删除 ISAKMP SA 请求。

第二步：发起方应该清除连接状态，进入 CLOSED 状态。若不是，则发起方行为不符合 IKEv1 协议规范要求。

7.8.1.4 响应方行为测试

测试 IKEv1 协议在野蛮模式交换情况下响应方的行为（其行为状态见附录 B 的 B.2.2.6），测试步骤如下：

a） START 状态测试

START 状态测试步骤如下：

1） 正常情况

第一步：发送消息 1，查看响应方的行为。

第二步：查看接收到的消息是否为消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

第三步：查看消息 2 结构是否合法，参数是否正确。若不合法，则响应方行为行为不符合 IKEv1 协议规范要求。

第四步：验证消息 2 中的签名、HASH 值是否正确。若不正确，则响应方行为行为不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：发送消息 1 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 提供非法参数

第一步：在消息 1 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 错误消息

第一步：在消息 1 中包含非法的载荷类型。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

b） AGGR_R1 状态测试

AGGR_R1 状态测试步骤如下：

1） 正常情况

第一步：发送消息 3，查看响应方的行为。

第二步：响应方应协商完成，进入连接状态。

2） 非期望消息

第一步：发送消息 3 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 3。

第二步：响应方应超时重传消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 3 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 3 中包含非法载荷类型。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 3，直到响应方的重传计数器值超过指定的最大值。

第二步：响应方应该清除状态，终止协商。若不是，则响应方行为不符合 IKEv1 协议规范要求。

c） AGGR_R2 状态测试

AGGR_R2 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态，阶段 1 协商完成。

第二步：准备开始阶段 2 的协商。

2） SA 管理

第一步：ISAKMP SA 到期或接收到删除 ISAKMP SA 请求。

第二步：响应方应该清除连接状态，进入 CLOSED 状态。若不是，则响应方行为不符合 IKEv1 协议规范要求。

7.8.2 性能测试

配置 IPsec 协议应用工作在 IKEv1 阶段 1 的野蛮模式交换方式，进行性能测试。测试步骤见7.7.2的规定。

7.8.3 健壮性测试

7.8.3.1 无效报文处理能力测试

测试 IKEv1 协议在野蛮模式交换情况下的无效报文处理能力，测试步骤如下：

a） 错误报文处理能力测试

在野蛮模式消息交换过程中发送错误报文，测试 IKEv1 协议的处理能力。测试步骤见7.8.1.3和 7.8.1.4 中各状态下提供非法参数测试步骤和错误消息测试步骤。

b） 非期望报文处理能力测试

在野蛮模式消息交换过程中发送非期望消息，测试 IKEv1 协议的处理能力。测试步骤见

7.8.1.3和7.8.1.4 中各状态下非期望消息的测试步骤。

7.8.3.2 异常事件处理能力测试

测试 IKEv1 协议在野蛮模式交换情况下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

配置 IPsec 协议应用触发 IKEv1 野蛮模式交换，进行连接中断处理能力测试。测试步骤见7.7.3.2a)。

b) 等待超时处理能力测试

配置 IPsec 协议应用触发 IKEv1 野蛮模式交换，在交换过程中延长数据交互时间直到超时，测试 IKEv1 协议的处理能力。测试步骤见 7.8.1.3 和 7.8.1.4 中各状态下延迟发送测试步骤和重传计数器超过最大值的测试步骤。

7.8.3.3 高强度负载处理能力测试

测试 IKEv1 协议在野蛮模式交换情况下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

配置 IPsec 协议应用触发 IKEv1 野蛮模式交换，进行网络高强度负载处理能力测试。测试步骤见 7.7.3.3a)。

b) 系统高强度负载处理能力测试

配置 IPsec 协议应用触发 IKEv1 野蛮模式交换，进行系统高强度负载处理能力测试。测试步骤见 7.7.3.3b)。

7.8.4 互操作性测试

7.8.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv1 野蛮模式交换情况下，实现基本连通测试。测试步骤见7.1.1.1。

7.8.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 野蛮模式交换情况下，实现功能互操作性测试。测试步骤见 7.8.1.2 的规定。

7.8.4.3 行为互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 野蛮模式交换情况下，实现行为互操作性测试。测试步骤见 7.8.1.3 和 7.8.1.4 的规定。

7.9 IKEv1 快速模式测试步骤

7.9.1 功能测试

7.9.1.1 基本互连测试

配置 IPsec 协议应用工作在 IKEv1 快速模式交换阶段，进行基本互连测试。测试步骤见 7.7.1.1。

7.9.1.2 安全功能测试

测试 IKEv1 协议在快速模式交换情况下的安全功能，测试步骤如下：

a) 加密算法协商功能

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：查看消息 1 的 SA 中是否有加密属性载荷。若有，则发起方支持加密算法协商功能。

第三步：查看消息 2 的 SA 中是否有加密属性载荷。若有，则响应方支持密码算法协商功能。

第四步：查看协商好的 IPsec SA 中是否有数据加密算法。若有，则支持加密算法协商功能。

b) MAC 算法协商功能

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：查看消息 1 中是否有协商 MAC 算法的属性载荷。若有，则发起方支持 MAC 算法协商功能。

第三步：查看消息 2 中是否有协商 MAC 算法的属性载荷。若有，则响应方支持 MAC 算法协商功能。

第四步：查看协商好的 IPsec SA 中是否有 MAC 算法。若有，则支持 MAC 算法协商功能。

c) 密钥协商功能

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：查看消息 1 中是否有密钥交换载荷(可选)和 Nonce 载荷。若有，则支持密钥协商。

第三步：查看消息 2 中是否有密钥交换载荷(可选和 Nonce 载荷。若有，则支持密钥协商。

第四步：查看协商好的 IPsec SA 中密钥是否存在。若存在，则说明支持密钥协商功能。

d) NAT 穿越的原始地址交换功能

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：查看消息 1 中是否有 NAT-OA 载荷。若有，则发起方支持原始地址交换功能。

第三步：查看消息 2 中是否有 NAT-OA 载荷。若有，则响应方支持原始地址交换功能。

7.9.1.3 发起方行为测试

测试 IKEv1 协议在快速模式交换情况下发起方的行为(其行为状态见附录 B 的 B.2.3.2)，测试步骤如下)：

a) START 状态测试

第一步：利用阶段 1 的协商指示，或参数刷新要求，触发 IKEv1 进行快速模式交换。

第二步：查看接收到的消息是否为消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：验证消息 1 解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看消息 1 中载荷类型是否正确，该消息结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

b) QUICK_I1 状态测试

QUICK_I1 状态测试步骤如下：

1) 正常情况

第一步：发送消息 2，查看发起方的行为。

第二步：查看接收到的消息是否发送消息 3。若不是，则发起方行为不符合 IKEv1 协议规范要求。

第三步：验证消息 3 解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看消息 3 中载荷类型是否正确，该消息结构是否合法。若不合法，则发起方行为不符合 IKEv1 协议规范要求。

2) 非期望消息

第一步：发送消息 2 以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 2。

第二步：发起方应超时重传消息 1。若不是，则发起方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 2 中提供非法参数（如头部 HDR 中设置不同于消息 1 的版本号、加密标志未置位，载荷包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 2 中包含非法的载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 2，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv1 协议规范要求。

c） QUICK_I2 状态测试

QUICK_I2 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态。

第二步：将协商完成的参数传递给 IPsec 安全协议（如 AH 或 ESP）。

2） SA 管理

第一步：IPsec SA 到期或接收到删除 IPsec SA 请求。

第二步：发起方应该清除连接状态，进入 CLOSED 状态。若不是，则发起方行为不符合 IKEv1 协议规范要求。

7.9.1.4 响应方行为测试

测试 IKEv1 协议在快速模式交换情况下响应方的行为（其行为状态见附录 B 的 B.2.3.3），测试步骤如下：

a） START 状态测试

START 状态测试步骤如下：

1） 正常情况

第一步：发送消息 1，查看响应方的行为。

第二步：查看接收到的消息是否为消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

第三步：验证消息 2 解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看消息 2 中载荷类型是否正确，该消息结构是否合法，参数是否正确。若不合法，则响应方行为不符合 IKEv1 协议规范要求。

2） 非期望消息

第一步：发送消息 1 以外的其他消息。

第二步：响应方应该拒绝该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 提供非法参数

第一步：在消息 1 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号、加密标志未置位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 错误消息

第一步：在消息 1 中包含非法载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

b） QUICK_R1 状态测试

QUICK_R1 状态测试步骤如下：

1） 正常情况

第一步：发送消息 3，查看响应方的动作。

第二步：响应方应协商完成，进入连接状态。

2） 非期望消息

第一步：发送消息 3 以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

3） 延迟发送

第一步：延迟发送消息 3。

第二步：响应方应超时重传消息 2。若不是，则响应方行为不符合 IKEv1 协议规范要求。

4） 提供非法参数

第一步：在消息 3 中提供非法参数（如消息头部 HDR 中设置不同于消息 1 的版本号、加密标志未置位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

5） 错误消息

第一步：在消息 3 中包含非法载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv1 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送消息 3，直到响应方的重传计数器值超过指定的最大值。

第二步：响应方应该清除状态，终止协商。若不是，则响应方行为不符合 IKEv1 协议规范要求。

7.9.1.4.1 QUICK_R2 状态测试

QUICK_R2 状态测试步骤如下：

a） 正常情况

第一步：设置连接状态。

第二步：将协商完成的参数传递给 IPsec 安全协议（如 AH 或 ESP）。

b） SA 管理

第一步：IPsec SA 到期或接收到删除 IPsec SA 请求。

第二步：响应方应该清除连接状态，进入 CLOSED 状态。若不是，则响应方行为不符合 IKEv1 协议规范要求。

7.9.2 性能测试

测试 IKEv1 在快速模式交换情况下的性能指标，测试步骤如下：

a） 连接建立时延

第一步：配置 IPsec 协议应用，设置为支持 PFS，触发 IKEv1 快速模式交换。

第二步：统计快速模式连接建立时延。

第三步：配置 IPsec 协议应用，设置为不支持 PFS，触发 IKEv1 快速模式交换。

第四步：统计快速模式连接建立时延。

b) 单位时间新建连接数

第一步：配置 IPsec 协议应用，设置为支持 PFS。

第二步：发起方产生多个连接请求，测试单位时间内成功建立的连接数。

第三步：配置 IPsec 协议应用，设置为不支持 PFS。

第四步：发起方产生多个连接请求，测试单位时间内成功建立的连接数。

c) 设备支持的总连接数

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：发起方持续产生连接请求，保持建立的连接不释放。

第三步：在响应方不能接受连接时统计已经成功建立的阶段 2 连接数。

d) 剩余错误比率

第一步：配置 IPsec 协议应用，设置 IKEv1 为快速模式交换，并多次建立连接，传送数据，然后关闭连接。

第二步：统计在此过程中传送不正确、丢失或者重复的数据量和有效的数据量之比。

e) 失败概率

第一步：配置 IPsec 协议应用，设置 IKEv1 为支持 PFS 的快速模式交换，并多次建立连接、传送数据，然后关闭连接。

第二步：统计在此过程中的连接建立失败概率和传送失败概率。

第三步：配置 IPsec 协议应用，设置 IKEv1 为不支持 PFS 的快速模式交换，并多次建立连接、传送数据，然后关闭连接。

第四步：统计在此过程中的连接建立失败概率和传送失败概率。

f) 密钥更新

第一步：配置 IPsec 协议应用，设置 IPsec SA 的更新周期(如 1 h)，触发 IKEv1 建立连接，保持连接。

第二步：在指定时间间隔(如 1 h)后查看 IKEv1 协商情况，是否已经触发 IKEv1 快速模式交换更新密钥。

第三步：若未更新密钥，则不支持密钥更新功能。

7.9.3 健壮性测试

7.9.3.1 无效报文处理能力测试

测试 IKEv1 协议在快速模式交换情况下的无效报文处理能力，测试步骤如下：

a) 错误报文处理能力测试

在快速模式消息交换过程中发送错误报文，测试 IKEv1 的处理能力。测试步骤见 7.9.1.3 和 7.9.1.4 中各状态下提供非法参数测试步骤和错误消息测试步骤。

b) 非期望报文处理能力测试

在快速模式消息交换过程中发送非期望消息，测试 IKEv1 的处理能力。测试步骤见 7.9.1.3 和 7.9.1.4 中各状态下非期望消息的测试步骤。

7.9.3.2 异常事件处理能力测试

测试 IKEv1 协议在快速模式交换情况下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

第一步：配置 IPsec 协议应用，触发 IKEv1 快速模式交换。

第二步：断开物理网络连接。

第三步：IKEv1 应该重传报文，直到达到最大重传计数值，终止协商。

b) 等待超时处理能力测试

在快速模式消息交换过程中延长数据交互时间直到超时，测试 IKEv1 协议的处理能力。测试步骤见 7.9.1.3 和 7.9.1.4 中各状态下延迟发送测试步骤和重传计数器超过最大值的测试步骤。

7.9.3.3 高强度负载处理能力测试

测试 IKEv1 协议在快速模式交换情况下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：在网络负载很大(带宽占用率为 90%以上)的情况下，触发 IKEv1 快速模式交换。

第二步：查看 IKEv1 的处理能力。

b) 系统高强度负载处理能力测试

第一步：在系统高强度负载(内存、CPU 占用率为 90%以上)的情况下，触发 IKEv1 快速模式交换。

第二步：查看 IKEv1 的处理能力。

7.9.4 互操作性测试

7.9.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv1 快速模式交换情况下，进行基本连通测试。测试步骤见 7.7.1.1。

7.9.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 快速模式交换情况下，进行功能互操作性测试。测试步骤见 7.9.1.2 的规定。

7.9.4.3 行为互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv1 快速模式交换情况下，进行行为互操作性测试。测试步骤见 7.9.1.3 和 7.9.1.4 的规定。

7.10 IKEv2 初始交换测试步骤

7.10.1 功能测试

7.10.1.1 基本互连测试

配置 IPsec 协议应用，触发 IKEv2 初始交换，进行基本互连测试。测试步骤见 7.7.1.1。

7.10.1.2 安全功能测试

测试 IKEv2 协议在初始交换情况下的安全功能，测试步骤如下：

a) 身份认证方法协商功能测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_SA_INIT 请求消息中的 SA 属性载荷部分。若没有认证方式的属性载荷，则不支持身份认证方法的协商功能。

第三步：查看 IKE_SA_INIT 响应消息中的 SA 属性载荷部分。若没有认证方式的属性载荷，则不支持身份认证方法的协商功能。

b) 身份认证功能测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_AUTH 请求消息中是否有认证载荷部分，且认证数据验证正确，则发起方具备身份认证功能。

第三步：查看 IKE_AUTH 响应消息中是否有认证载荷部分，且认证数据验证正确，则响应方具备身份认证功能。

c) 加密算法协商功能测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_SA_INIT 请求消息中是否有加密算法属性载荷。若有，则发起方支持加密算法协商功能。

第三步：查看 IKE_SA_INIT 响应消息中是否有加密算法载荷。若有，则响应方支持加密算法协商功能。

第四步：查看协商好的 IKE SA 中是否有加密算法标识。若有，则说明支持加密算法协商功能。

d) 伪随机函数 PRF 协商功能测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_SA_INIT 请求消息中是否有伪随机函数的属性载荷。若有，则发起方支持伪随机函数 PRF 协商功能。

第三步：查看 IKE_SA_INIT 响应消息中是否有伪随机函数的属性载荷。若有，则响应方支持伪随机函数 PRF 协商功能。

第四步：查看协商好的 IKE SA 中是否有伪随机函数 PRF 标识。若有，则说明支持伪随机函数 PRF 协商功能。

e) 密钥协商功能

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_SA_INIT 请求消息中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第三步：查看 IKE_SA_INIT 响应消息中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第四步：查看协商好的 IKE SA 中密钥是否存在。若存在，则说明支持密钥协商功能。

f) 数据加密功能测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：查看 IKE_AUTH 请求消息中是否有加密载荷。若有，则支持数据加密功能。

第三步：查看 IKE_AUTH 响应消息中是否有加密载荷。若有，则支持数据加密功能。

g) NAT 穿越探测功能

第一步：配置 IPsec 协议应用，触发 IKEv1 初始交换。

第二步：查看消息 1 中是否有 NAT_DETECTION_SOURCE_IP 和 NAT_DETECTION_DESTINATION_IP 类型的通知载荷。若有，则发起方支持 NAT 穿越功能。

第三步：查看消息 2 中是否有 NAT_DETECTION_SOURCE_IP 和 NAT_DETECTION_DESTINATION_IP 类型的通知载荷。若有，则响应方支持 NAT 穿越功能。

第四步：若 IPsec 协议应用的上述检查通过，则支持 NAT 穿越探测功能。

h） NAT KEEPALIVE 功能

第一步：配置 IPsec 协议应用，在连接中设置 NAT 设备，触发 IKEv2 初始交换。

第二步：检查是否收到 NAT KEEPALIVE 报文。若是，则方支持 NAT KEEPALIVE 功能。

第三步：NAT KEEPALIVE 报文的接收方应丢弃该报文。

7.10.1.3 发起方行为测试

测试 IKEv2 协议在初始交换情况下发起方的行为（其行为状态见附录 C 的 C.2.1.2），测试步骤如下：

a） START 状态测试

第一步：配置参数，触发发起方 IPsec 协议（如 AH 或 ESP）产生连接请求。

第二步：查看接收到的消息是否为 IKE_SA_INIT 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

第三步：查看 IKE_SA_INIT 请求消息结构是否合法。若不合法，则发起方行为不符合 IKEv2 协议规范要求。

b） INIT_I_REQ 状态测试

INIT_I_REQ 状态测试步骤如下：

1） 正常情况

第一步：发送 IKE_SA_INIT 响应消息，查看发起方的行为。

第二步：查看发起方是否发送 IKE_AUTH 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

第三步：查看 IKE_AUTH 请求消息解密是否正确，消息结构是否合法。若不合法，则发起方行为不符合 IKEv2 协议规范要求。

第四步：发送带 Cookie 的载荷的响应消息，查看发起方的行为。

第五步：查看是否接收到带 Cookie 载荷的 IKE_SA_INIT 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

第六步：查看带 Cookie 载荷的 IKE_SA_INIT 请求消息结构是否合法。若不合法，则发起方行为不符合 IKEv2 协议规范要求。

2） 非期望消息

第一步：发送 IKE_SA_INIT 响应消息以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

3） 延迟发送

第一步：延迟发送 IKE_SA_INIT 响应消息。

第二步：发起方应超时重传 IKE_SA_INIT 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

4） 提供非法参数

第一步：在 IKE_SA_INIT 响应消息中提供非法参数（如消息头部 HDR 中设置不同的版本号、将响应方 SPI 设置为 0，建议和变换载荷中提供不在协议规范中定义的参数值）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

5） 错误消息

第一步：在 IKE_SA_INIT 响应消息中包含非法的载荷类型。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送 IKE_SA_INIT 响应，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv2 协议规范要求。

c) INIT_I_COOKIE 状态测试

INIT_I_COOKIE 状态测试步骤如下：

1) 正常情况

第一步：发送 IKE_SA_INIT 响应消息，查看发起方的行为。

第二步：查看发起方是否发送 IKE_AUTH 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

第三步：验证 IKE_AUTH 请求消息解密是否正确。若不正确，则发起方行为不符合 IKEv2 协议规范要求。

第四步：查看 IKE_AUTH 请求消息的载荷类型是否正确，该消息结构是否合法。若不合法，则发起方行为不符合 IKEv2 协议规范要求。

2) 非期望消息

第一步：发送 IKE_SA_INIT 响应消息以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

3) 延迟发送

第一步：延迟发送 IKE_SA_INIT 响应消息。

第二步：发起方应超时重传带 Cookie 载荷的 IKE_SA_INIT 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

4) 提供非法参数

第一步：在 IKE_SA_INIT 响应消息中提供非法参数（如消息头部 HDR 中置不同的版本号、将响应方 SPI 设置为 0，建议和变换载荷中提供不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

5) 错误消息

第一步：在 IKE_SA_INIT 响应消息中包含非法的载荷类型。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

6) 重传计数器超过最大值

第一步：延迟发送 IKE_SA_INIT 响应，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv2 协议规范要求。

d) AUTH_I_REQ 状态测试

AUTH_I_REQ 状态测试步骤如下：

1) 正常情况

第一步：发送 IKE_AUTH 响应消息，查看发起方的行为。

第二步：发起方进入 ESTABLISHED 状态。

2) 非期望消息

第一步：发送 IKE_AUTH 响应消息以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

3) 延迟发送

第一步：延迟发送 IKE_AUTH 响应消息。

第二步：发起方应超时重传 IKE_AUTH 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

4） 提供非法参数

第一步：在 IKE_AUTH 响应消息中提供非法参数（如头部 HDR 中设置不同于 IKE_AUTH 请求消息的版本号、将响应方 SPI 设置为 0、头部之后不是加密载荷，载荷中包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

5） 错误消息

第一步：在 IKE_AUTH 响应消息中包含非法的载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送 IKE_AUTH 响应，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv2 协议规范要求。

e） ESTABLISHED 状态测试

ESTABLISHED 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态，初始交换完成。

第一步：构建 IKE SA 连接状态，并将协商好的 IPsec SA 传递给协议（如 AH 或 ESP）。

2） SA 管理

第一步：IKE SA 到期或接收到删除 IKE SA 请求。

第二步：发起方应该清除连接状态，进入 CLOSED 状态。若不是，则发起方行为不符合 IKEv2 协议规范要求。

7.10.1.4 响应方行为测试

测试 IKEv2 协议在初始交换情况下响应方的行为（其行为状态见附录 C 的 C.2.1.3），测试步骤如下：

a） START 状态测试

START 状态测试步骤如下：

1） 正常情况处理能力测试

第一步：发送 IKE_SA_INIT 请求消息，测试响应方的行为。

第二步：查看接收到的消息是否为 IKE_SA_INIT 响应消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

第三步：查看 IKE_SA_INIT 响应消息结构是否合法。若不合法，则响应方行为不符合 IKEv2 协议规范要求。

第四步：持续以不同的身份发送 IKE_SA_INIT 请求消息，直到响应方半打开连接达到最大值。

第五步：查看接收到的消息是否为带 Cookie 载荷的响应消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

第六步：查看带 Cookie 载荷的响应消息是否合法。若不合法，则响应方行为不符合 IKEv2 协议规范要求。

2） 非期望消息

第一步：发送 IKE_SA_INIT 请求消息以外的其他消息。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

3） 提供非法参数

第一步：在 IKE_SA_INIT 请求消息中提供非法参数（如消息的 HDR 中设置不同的版本号，建议和变换载荷中提供不在协议规范中定义的参数值等）。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

4） 错误消息

第一步：在 IKE_SA_INIT 请求消息中包含非法载荷类型。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

b） INIT_R_REQ 状态测试

INIT_R_REQ 状态测试步骤如下：

1） 正常情况处理能力测试

第一步：发送 IKE_AUTH 请求消息，测试响应方的行为。

第二步：查看是否接收到 IKE_AUTH 响应消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

第三步：验证 IKE_AUTH 响应消息解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看 IKE_AUTH 响应消息载荷类型是否正确，消息结构是否合法、是否提供认证载荷。若不是，则响应方行为不符合 IKEv2 协议规范要求。

2） 非期望消息

第一步：发送 IKE_AUTH 请求消息以外的其他消息。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

3） 提供非法参数

第一步：在 IKE_AUTH 请求消息中提供非法参数（如 HDR 中设置不同的版本号、标志位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

4） 错误消息

第一步：在 IKE_AUTH 请求消息中包含非法的载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

c） INIT_R_COOKIE 状态测试

INIT_R_COOKIE 状态测试步骤如下：

1） 正常情况处理能力测试

第一步：发送带 Cookie 载荷的 IKE_SA_INIT 请求消息，测试响应方的行为。

第二步：查看响应方是否发送 IKE_SA_INIT 响应消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

第三步：查看 IKE_SA_INIT 响应消息结构是否合法。若不是，则响应方行为不符合 IKEv2 协议规范要求。

2） 非期望消息

第一步：发送带 Cookie 载荷的 IKE_SA_INIT 请求消息以外的其他消息。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

3） 提供非法参数

第一步：在带 Cookie 载荷的 IKE_SA_INIT 请求消息中提供非法参数（如该消息 HDR 中设置不同的版本号、标志位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

4） 错误消息

第一步：在带 Cookie 载荷的 IKE_SA_INIT 请求消息中包含非法的载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：响应方应丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

d） ESTABLISHED 状态测试

ESTABLISHED 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态，初始交换完成。

第二步：构建 IKE SA 连接状态，并将协商好的 IPsec SA 传递给协议（如 AH 或 ESP）。

2） SA 管理

第一步：IKE SA 到期或接收到删除 IKE SA 请求。

第二步：响应方应该清除连接状态，进入 CLOSED 状态。若不是，则响应方行为不符合 IKEv2 协议规范要求。

7.10.2 性能测试

配置 IPsec 协议应用触发 IKEv2 初始交换，进行性能测试。测试步骤见 7.7.2。

7.10.3 健壮性测试

7.10.3.1 无效报文处理能力测试

测试 IKEv2 协议在初始交换情况下的无效报文处理能力，测试步骤如下：

a） 错误报文处理能力测试

在初始交换过程中发送错误报文，测试 IKEv2 协议的处理能力。测试步骤见 7.10.1.3 和 7.10.1.4中各状态下提供非法参数测试步骤和错误消息测试步骤。

b） 非期望报文处理能力测试

在初始交换过程中发送非期望消息，测试 IKEv2 协议的处理能力。测试步骤见 7.10.1.3 和 7.10.1.4 中各状态下非期望消息的测试步骤。

7.10.3.2 异常事件处理能力测试

测试 IKEv2 协议在初始交换情况下的异常事件处理能力，测试步骤如下：

a） 连接中断处理能力测试

第一步：配置 IPsec 协议应用，触发 IKEv2 初始交换。

第二步：断开物理网络连接。

第三步：IKEv2 发起方应该重传报文，直到达到最大重传计数值，终止协商。

b） 等待超时处理能力测试

在初始交换过程中延长数据交互时间直到超时，测试 IKEv2 协议的处理能力。测试步骤见 7.10.1.3和 7.10.1.4 中各状态下延迟发送测试步骤和重传计数器超过最大值的测试步骤。

7.10.3.3 高强度负载处理能力测试

测试 IKEv2 协议在初始交换情况下的高强度负载处理能力，测试步骤如下：

a） 网络高强度负载处理能力测试

第一步：在网络负载很大（带宽占用率为 90％以上）的情况下，触发 IKEv2 初始交换。

第二步：查看 IKEv1 的处理能力。

b） 系统高强度负载处理能力测试

第一步：在系统高强度负载（内存、CPU 占用率为 90％以上）的情况下，触发 IKEv2 初始交换。

第二步：查看 IKEv1 的处理能力。

7.10.4 互操作性测试

7.10.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv2 初始交换情况下，进行基本连通测试。测试步骤见 7.7.1.1。

7.10.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv2 初始交换情况下，进行功能互操作性测试。测试步骤见 7.10.1.2 的规定。

7.10.4.3 行为互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv2 初始交换情况下，进行行为互操作性测试。测试步骤见 7.10.1.3 和 7.10.1.4 的规定。

7.11 IKEv2 创建子 SA 交换测试步骤

7.11.1 功能测试

7.11.1.1 基本互连测试

配置 IPsec 协议应用，触发 IKEv2 创建子 SA 交换过程，进行基本互连测试。测试步骤见 7.7.1.1。

7.11.1.2 安全功能测试

测试 IKEv2 协议在创建子 SA 交换情况下的安全功能，测试步骤如下：

a） 加密算法协商功能

第一步：配置 IPsec 协议应用，触发 IKEv2 创建子 SA 交换。

第二步：查看 CREATE_CHILD_SA 请求消息中是否有加密算法属性载荷。若有，则支持加密算法协商功能。

第三步：查看 CREATE_CHILD_SA 响应消息中是否有加密算法属性载荷。若有，则支持密码算法协商功能。

第四步：查看协商好的 CHILD SA 中是否有数据加密算法标识。若有，则说明支持加密算法协商功能。

b） MAC 算法协商功能

第一步：配置 IPsec 协议应用，触发 IKEv2 创建子 SA 交换。

第二步：查看 CREATE_CHILD_SA 请求消息中是否有 MAC 算法协商的属性载荷。若有，则支持 MAC 算法协商功能。

第三步：查看 CREATE_CHILD_SA 响应消息中是否有 MAC 算法协商的属性载荷。若有，则支持 MAC 算法协商功能。

第四步：查看协商好的 CHILD SA 中否有 MAC 算法标识。若有，则支持 MAC 算法协商功能。

c) 密钥协商功能

第一步：配置 IPsec 协议应用，触发 IKEv2 创建子 SA 交换。

第二步：查看 CREATE_CHILD_SA 请求中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第三步：查看 CREATE_CHILD_SA 响应消息中是否有密钥交换载荷和 Nonce 载荷。若有，则支持密钥协商功能。

第四步：查看协商好的 CHILD SA 中密钥是否存在。若存在，则说明支持密钥协商功能。

d) 密钥更新功能

第一步：配置 IPsec 协议应用，触发 IKEv2 创建子 SA 交换。

第二步：查看 CREATE_CHILD_SA 请求中是否有通知载荷（包含 SPI 值）和业务流选择载荷，确定是否支持密钥更新功能。

第三步：查看 CREATE_CHILD_SA 响应消息中是否有通知载荷（包含 SPI 值）和业务流选择载荷，确定是否支持密钥协商功能。

第四步：查看协商好的 CHILD SA 中密钥是否被更新。

7.11.1.3 发起方行为测试

测试 IKEv2 协议在创建子 SA 交换情况下发起方的行为（其行为状态见附录 C 的 C.2.2.2），测试步骤如下：

a) START 状态测试

第一步：利用 IKEv2 初始交换的协商指示，或收到参数刷新要求，触发 IKEv2 进行创建子 SA 交换。

第二步：查看接收到的消息是否为 CREATE_CHILD_SA 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

第三步：验证 CREATE_CHILD_SA 请求消息解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看 CREATE_CHILD_SA 请求消息载荷类型是否正确，消息结构是否合法。若不合法，则发起方行为不符合 IKEv2 协议规范要求。

b) CHILD_I_REQ 状态测试

CHILD_I_REQ 状态测试步骤如下：

1) 正常情况

第一步：发送 CREATE_CHILD_SA 响应消息，查看发起方的行为。

第二步：发起方应指示协商完成，进入 ESTABLISHED 状态。

2) 非期望消息

第一步：发送 CREATE_CHILD_SA 响应消息以外的其他消息。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

3) 延迟发送

第一步：延迟发送 CREATE_CHILD_SA 响应消息。

第二步：发起方应超时重传 CREATE_CHILD_SA 请求消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

4) 提供非法参数

第一步：在 CREATE_CHILD_SA 响应消息中提供非法参数（如头部 HDR 中设置不同的版本号、响应方 Cookie 设置为 0，载荷包含不在协议规范中定义的参数值等）。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

5） 错误消息

第一步：在 CREATE_CHILD_SA 响应消息中包含非法载荷类型或使用协商结果以外的算法和密钥加密报文。

第二步：发起方应该丢弃该消息。若不是，则发起方行为不符合 IKEv2 协议规范要求。

6） 重传计数器超过最大值

第一步：延迟发送 CREATE_CHILD_SA 响应，直到发起方的重传计数器值超过指定的最大值。

第二步：发起方应该清除状态，终止协商。若不是，则发起方行为不符合 IKEv2 协议规范要求。

c） ESTABLISHED 状态测试

ESTABLISHED 状态测试步骤如下：

1） 正常情况

第一步：设置连接状态。

第二步：将协商完成的参数传递给 IPsec 安全协议（如 AH 或 ESP）。

2） SA 管理

第一步：IPsec SA 到期或接收到删除 IPsec SA 请求。

第二步：发起方应该清除连接状态，进入 CLOSED 状态。若不是，则发起方行为不符合 IKEv2 协议规范要求。

7.11.1.4 响应方行为测试

测试 IKEv2 协议在创建子 SA 交换情况下响应方的行为（其行为状态见附录 C 的 C.2.2.3），测试步骤如下：

a） START 状态测试

START 状态测试步骤如下：

1） 正常情况

第一步：发送 CREATE_CHILD_SA 请求消息，查看响应方的行为。

第二步：查看接收到的消息是否为 CREATE_CHILD_SA 响应消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

第三步：验证 CREATE_CHILD_SA 响应消息解密是否正确。若不正确，则发起方行为不符合 IKEv1 协议规范要求。

第四步：查看 CREATE_CHILD_SA 响应消息载荷类型是否正确，消息结构是否合法。若不合法，则响应方行为不符合 IKEv2 协议规范要求。

2） 非期望消息

第一步：发送 CREATE_CHILD_SA 请求消息以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

3） 提供非法参数

第一步：在 CREATE_CHILD_SA 请求消息中提供非法参数（如消息头部 HDR 中设置非法参数，如设置不同于消息 1 的版本号、标志位，载荷包含不在协议规范中定义的参数值等）。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

4） 错误消息

第一步：在 CREATE_CHILD_SA 请求消息中包含非法的载荷类型或使用协议结果以外的算法和密钥加密报文。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

b） CHILD_R_REQ 状态测试

CHILD_R_REQ 状态测试步骤如下：

1） 正常情况

第一步：计算参数，设置协商完成状态。

第二步：进入 ESTABLISHED 状态。

2） 非期望消息

第一步：发送 CREATE_CHILD_SA 请求消息以外的其他消息。

第二步：响应方应该丢弃该消息。若不是，则响应方行为不符合 IKEv2 协议规范要求。

c） ESTABLISHED 状态测试

1） 正常情况

第一步：设置连接状态。

第二步：将协商完成的参数传递给 IPsec 安全协议（如 AH 或 ESP）。

2） SA 管理

第一步：IPsec SA 到期或接收到删除 IPsec SA 请求。

第二步：响应方应该清除连接状态，进入 CLOSED 状态。若不是，则响应方行为不符合 IKEv2 协议规范要求。

7.11.2 性能测试

测试 IKEv2 协议在创建子 SA 交换情况下的性能指标，测试步骤见 7.9.2 的规定。

7.11.3 健壮性测试

7.11.3.1 无效报文处理能力测试

测试 IKEv2 协议在创建子 SA 交换情况下的无效报文处理能力，测试步骤如下：

a） 错误报文处理能力测试

在创建子 SA 交换过程中发送错误报文，测试 IKEv2 的处理能力。测试步骤见 7.11.1.3 和 7.11.1.4 中各状态下提供非法参数测试步骤和错误消息测试步骤。

b） 非期望报文处理能力测试

在创建子 SA 交换过程中发送非期望消息，测试 IKEv2 的处理能力。测试步骤见 7.11.1.3 和 7.11.1.4 中各状态下非期望消息的测试步骤。

7.11.3.2 异常事件处理能力测试

测试 IKEv2 协议在创建子 SA 交换情况下的异常事件处理能力，测试步骤如下：

a） 连接中断处理能力测试

第一步：配置 IPsec 协议应用，触发创建子 SA 交换协商。

第二步：断开物理网络连接。

第三步：IKEv2 发起方应该重传报文，直到达到最大重传计数值，终止协商。

b） 等待超时处理能力测试

在创建子 SA 交换过程中延长数据交互时间直到超时，测试 IKEv2 协议的处理能力。测试步骤见 7.11.1.3 和 7.11.1.4 中各状态下延迟发送测试步骤和重传计数器超过最大值的测试步骤。

7.11.3.3 高强度负载处理能力测试

测试 IKEv2 协议在创建子 SA 交换情况下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：在网络负载很大(带宽占用率为 90%以上)的情况下，触发创建子 SA 交换过程。

第二步：查看 IKEv2 的处理能力。

b) 系统高强度负载处理能力测试

第一步：在系统高强度负载(内存、CPU 占用率为 90%以上)的情况下，触发创建子 SA 交换过程。

第二步：查看 IKEv2 的处理能力。

7.11.4 互操作性测试

7.11.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv2 创建子 SA 交换情况下，实现基本连通测试。测试步骤见 7.7.1.1。

7.11.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv2 创建子 SA 交换情况下，进行功能互操作性测试。测试步骤见 7.11.1.2 的规定。

7.11.4.3 行为互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv2 创建子 SA 交换情况下，进行行为互操作性测试。测试步骤见 7.11.1.3 和 7.11.1.4 的规定。

7.12 IKEv2 信息交换测试步骤

7.12.1 功能测试

7.12.1.1 基本互连测试

配置 IPsec 协议应用，触发 IKEv2 信息交换，进行基本互连测试。测试步骤见 7.7.1.1。

7.12.1.2 安全功能测试

测试 IKEv2 协议在信息交换情况下的安全功能，测试步骤如下：

a) 事件通知测试

第一步：发起方发送 INFORMATIONAL 请求消息，该消息中包含通知载荷，指定传递的事件。

第二步：响应方检查 INFORMATIONAL 请求消息，解密并获得通知载荷的内容。若解密不成功，则在信息交换下，发起方行为不符合 IKEv2 协议规范要求。

第三步：响应方按照事件通知执行相关动作并返回响应。

b) 删除安全关联测试

第一步：发起方发送 INFORMATIONAL 请求消息，该消息中包含删除载荷，指定了需要删除的 SA。

第二步：响应方检查 INFORMATIONAL 请求消息，解密并获得删除载荷的内容。若解密成

功，响应方删除载荷中指定的 SA；若解密不成功，则在信息交换下，发起方行为不符合 IKEv2 协议规范要求。

第三步：响应方返回 INFORMATIONAL 响应消息，该消息中包含删除载荷，指定了需要删除的 SA。

第四步：发起方检查 INFORMATIONAL 请求消息，解密并获得删除载荷的内容。若解密成功，发起方删除载荷中指定的 SA；若解密不成功，则在信息交换下，响应方行为不符合 IKEv2 协议规范要求。

c) 配置参数测试

第一步：发起方发送 INFORMATIONAL 请求消息，该消息中包含配置载荷，指定了需要配置的参数。

第二步：响应方检查 INFORMATIONAL 请求消息，解密并获得配置载荷的内容。若解密不成功，则在信息交换下，发起方行为不符合 IKEv2 协议规范要求。

第三步：响应方根据配置载荷中的参数进行网络等相关配置工作并返回响应。

d) 活性探测测试

第一步：发起方发送 INFORMATIONAL 请求消息，消息中不包含载荷。

第二步：响应方检查 INFORMATIONAL 请求消息。

第三步：响应方更新活性检测的计时器并返回响应。

7.12.2 性能测试

测试 IKEv2 协议在信息交换情况下的性能指标，测试步骤如下：

a) 剩余错误比率

第一步：配置 IPsec 协议应用，多次触发 IKEv2 传送 INFORMATIONAL 请求和响应消息。

第二步：统计在此过程中传送不正确、丢失或者重复的数据量和有效的数据量之比。

b) 失败概率

第一步：配置 IPsec 协议应用，多次触发 IKEv2 传送 INFORMATIONAL 请求和响应消息。

第二步：统计在此过程中的传递 INFORMATIONAL 消息失败概率。

7.12.3 健壮性测试

7.12.3.1 错误报文处理能力测试

第一步：触发 IKEv2 产生 INFORMATIONAL 交换。

第二步：构造 INFORMATIONAL 消息，消息的载荷中提供不在协议规范中定义的参数值、构建错误的 INFORMATIONAL 响应消息（如 HDR 中设置非法参数、设置不同的版本号、响应方 Cookie 设置为 0 等），并发送给对方。

第三步：上述错误报文该被丢弃。

7.12.3.2 异常事件处理能力测试

测试 IKEv1 协议在信息交换情况下的异常事件处理能力，测试步骤如下：

a) 连接中断处理能力测试

第一步：在 INFORMATIONAL 交换协商情况下，断开物理网络连接。

第二步：发起方应该重传报文，直到达到最大重传计数值。

b) 等待超时处理能力测试

第一步：在 INFORMATIONAL 交换协商情况下，响应方延长数据交互时间。

第二步：发起方应该超时重传报文。

7.12.3.3 高强度负载处理能力测试

测试 IKEv1 协议在信息交换情况下的高强度负载处理能力，测试步骤如下：

a) 网络高强度负载处理能力测试

第一步：在网络负载很大(带宽占用率为 90%以上)的情况下，触发 INFORMATIONAL 交换过程。

第二步：查看 IKEv2 的处理能力。

b) 系统高强度负载处理能力测试

第一步：在系统高强度负载(内存、CPU 占用率为 90%以上)的情况下，触发 INFORMATIONAL 交换过程。

第二步：查看 IKEv2 的处理能力。

7.12.4 互操作性测试

7.12.4.1 基本互连测试

设置不同 IPsec 协议应用均工作在 IKEv2 INFORMATIONAL 交换情况下，实现基本连通测试。测试步骤见 7.7.1.1。

7.12.4.2 功能互操作性测试

设置不同 IPsec 协议应用均工作在 IKEv2 INFORMATIONAL 交换情况下，实现功能互操作性测试。测试步骤见 7.12.1.2 的规定。

附 录 A
（资料性附录）
IPsec 协议规范说明

A.1 概述

IPsec 是将安全机制引入 TCP/IP 网络的一系列标准，可为 IPv4 和 IPv6 数据报提供高质量的、可互操作的、基于密码的安全服务。IPsec 在 IP 层提供访问控制、数据完整性验证、数据源认证、抗重放攻击、保密性以及有限业务流的保密性等安全服务。

IPsec 通过两个协议（如认证头协议 AH 和封装安全载荷协议 ESP）以及因特网密钥交换协议 IKE 提供安全服务。各协议功能如下：

a） AH 为 IP 数据报提供数据源认证、数据完整性校验以及抗重放攻击服务；

b） ESP 为 IP 数据报提供数据的保密性、数据源认证、数据完整性校验和抗重放攻击服务；

c） IKE（包括 IKEv1 和 IKEv2）完成身份认证、安全关联建立和安全参数协商等功能。

A.2 安全关联

A.2.1 安全策略数据库

IPsec 对数据流的保护由安全策略数据库 SPD 确定。SPD 定义了哪些服务以何种方式提供给 IP 数据报。安全策略数据库则根据数据流分类对报文作出 3 种处理：旁路、丢弃和应用 IPsec。旁路指允许数据通过但不提供 IPsec 保护；丢弃指不允许数据穿越 IPsec 设备；应用 IPsec 指对数据提供 IPsec 保护，此时 SPD 应该指出对数据流提供的安全服务、采用的协议、使用的算法等。

对于 IPsec 协议实现，应提供一个管理接口，该接口允许用户或系统管理员管理 SPD。管理接口应允许用户定义进入或离开系统的数据流处理方法。

SPD 包括一个有序的策略入口表。策略入口由一个或多个选择符标识，这些选择符定义了哪些数据流应该应用该策略。每个入口包括一个标识，该标识指出匹配这一策略的通信是否允许旁路、丢弃或应用 IPsec 处理。若需要进行 IPsec 处理，则入口应包括一个 SA 或 SA 束，给出了 IPsec 协议类型、模式和使用的算法，以及是否需要嵌套使用 SA 等。安全策略数据库是通过“选择符”来指定的，因此选择符成为安全策略数据库的索引。选择符是从网络层和传送层内提取出来的，它包含有下列字段：

a） 目标地址：该字段可以是一个指定的 IP 单播地址、一个地址范围（包括地址高值和低值）、地址加掩码或一个通配符地址。

b） 源地址：该字段可以是一个指定的 IP 单播地址、一个地址范围（包括地址高值和低值）、地址加掩码或一个通配符地址。

c） 名字：该字段用于标识与一名有效用户或者系统名称关联在一起的名称。可使用 DNS 域名、X.509 区分名或者在 IPsec DOI 中定义的其他名字类型。

d） 协议：该字段指定了传输层协议，从 IPv4 的协议字段或 IPv6 的下一个头字段得到。

e） 上层端口：在进行面向会话的密钥交换时，上层端口代表着源和目标端口，真正应用协议使用的就是这些端口。若端口不能访问（如接收到一个具有 ESP 头的报文），则需使用通配符。

A.2.2 安全关联数据库

安全关联类似于一条单向逻辑“连接”，输入数据流和输出数据流由输入安全关联和输出安全关联

分别处理。可通过手工配置和自动协商两种方式建立，但都是基于安全策略数据库生成的。自动协商方式就是由通信双方基于各自的安全策略数据库经过匹配和协商，最终建立安全关联。

对于入站处理，SAD 中的每个入口根据一个目的 IP 地址、IPsec 协议类型、SPI 进行检索。对于入站，下面的字段用于在 SAD 中查找 SA：

a) 外部头中的目的 IP 地址：对传输模式，是通信的目的地；对隧道模式，是隧道的目的端点。

b) IPsec 安全协议：AH 或 ESP 协议，用于作为查找安全关联的索引，指定了该安全关联使用的协议类型。

c) SPI：用于区分同一目的地址和安全协议的情况下不同的安全关联。

对于每个选择符，SAD 中的 SA 入口应包含一个或多个在创建 SA 时协商的值。对于发起方，这些值用于决定哪个 SA 应该被使用；对于响应方，这些值用于核对入站报文中的选择符值与 SA 的选择符值是否一致。下述 SA 字段用在 IPsec 处理过程中：

a) 序号计数：产生 AH 或 ESP 头中的序号字段，主要用于抗重放攻击服务。

b) 序号溢出：指示序号计数器的溢出是否应该产生一个日志记录，并且阻止用该 SA 继续传输分组。

c) 抗重放窗口：包括一个计数器和一个检测窗口，用于判断一个输入的 AH 或 ESP 报文是否为重放报文。

d) AH 认证算法、密钥。

e) ESP 加密算法、密钥、Ⅳ模式和Ⅳ。

f) ESP 认证算法、密钥，若没有使用认证服务，则该字段设置为空。

g) 生存期：规定了每个 SA 最长能够存在的时间。超过这个时间，该 SA 便不能继续使用。可使用字节数和时间（按秒计算）为单位计算。

h) IPsec 协议模式：传输模式或隧道模式。

A.2.3 安全关联的组合

A.2.3.1 传输邻接组合模式

传输邻接指的是对同一个 IP 数据报使用多于一个传输模式的安全协议。这种联合 AH 和 ESP 的方法只允许一级的联合，更多的嵌套不能产生更多的好处。传输邻接组合模式如图 A.1 所示。

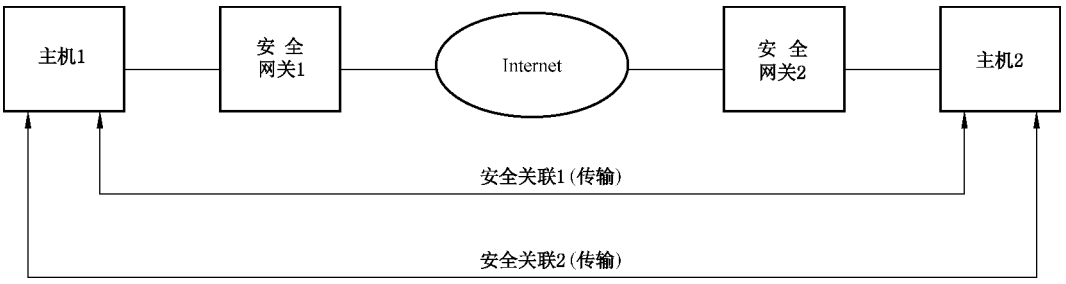


图 A.1 传输邻接组合模式

A.2.3.2 迭代隧道组合模式

迭代隧道指的是通过 IP 隧道实现的安全协议的多层次应用。这种方法允许多重嵌套。常见的有三种基本的嵌套隧道方式：

a) 隧道的两个端点相同（隧道的内部与外部均有可能是为 AH 或 ESP，如图 A.2 所示）；

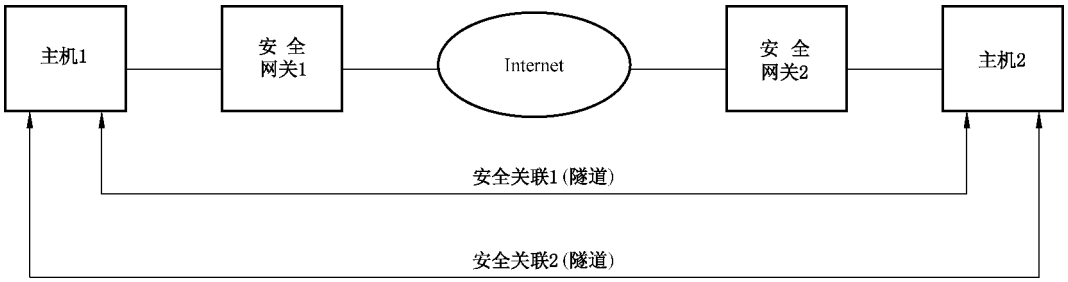


图 A.2　隧道端点相同的迭代隧道组合模式

b)　一个隧道端点相同(隧道的内部与外部均有可能是为 AH 或 ESP,如图 A.3 所示);

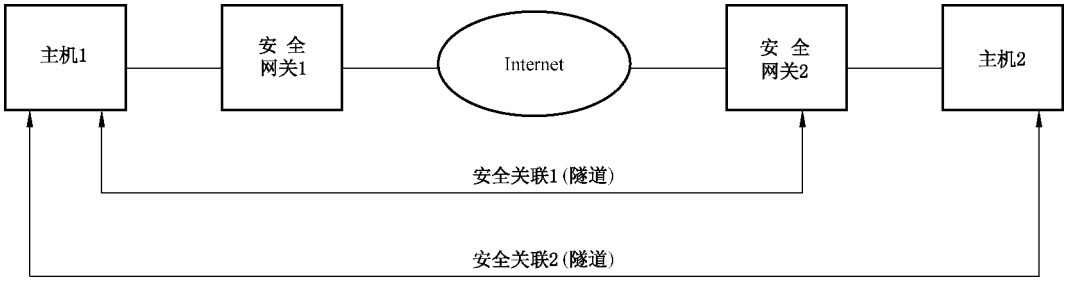


图 A.3　一个隧道端点相同的迭代隧道组合模式

c)　隧道端点均不相同(隧道的内部与外部均有可能是 AH 或 ESP,如图 A.4 所示)。

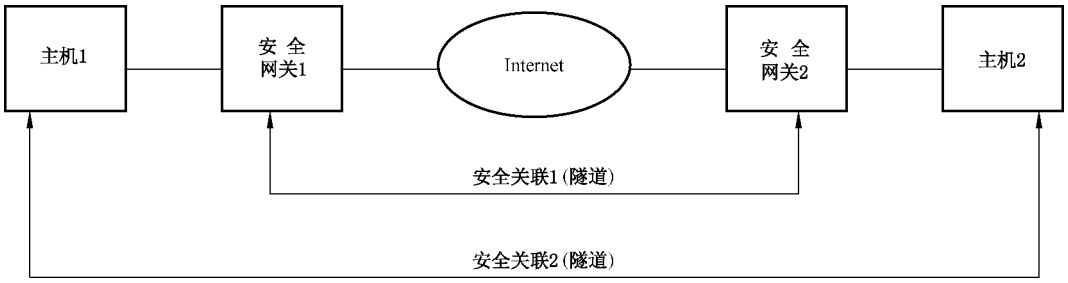


图 A.4　隧道端点均不相同的迭代隧道组合模式

A.2.4　安全关联的管理

SA 的管理既可以手工进行,也可以通过自动密钥管理协议(如 IKE)来完成。不同的方法会影响协议提供的安全服务,AH 和 ESP 协议独立于相关的 SA 管理技术。

手工 SA 管理可由管理员配置密钥,设置 SA 参数。手工方式静态配置适用于小规模的环境,并在有限范围内保护流量。在大规模的网络中应用 IPsec 时需要用到自动密钥管理协议 IKE。该协议在因特网上为两个设备自动协商安全参数。

SA 管理的主要任务是创建和删除。SA 的创建分为两步:首先协商 SA 参数,然后用 SA 更新 SAD。协议规范要求必须支持手工密钥管理机制,此时 SPI 的分配、参数的拟订均是手工完成的;同时应该支持自动密钥管理协议(如 IKE)完成参数的协商。若安全策略要求建立安全、保密的连接,却找不到相应的 SA,IPsec 会自动调用 IKE 创建该 SA,并添加到 SAD 数据库中。

当 SA 不能满足安全通信的要求时,必须删除。删除的条件为:生存期过期、密钥被破解、SA 加密/解密或验证的字节数超过了策略设定的阀值、另一端要求删除该 SA 等。

附 录 B
（资料性附录）
IKEv1 密钥交换机制

B.1 定义

IKEv1 是一个混合型的协议，利用 ISAKMP 定义的认证和密钥交换框架。密钥协商过程包括两个阶段，即阶段 1 和阶段 2。在阶段 1 中，应支持主模式交换和野蛮模式交换。在此阶段通信双方协商建立了一个 ISAKMP SA，该 SA 是为保护彼此之间的通信而使用的策略及密钥，用该 SA 协商的参数保护 IPsec SA 的协商过程。一个 ISAKMP SA 可用于建立多个 IPsec SA。阶段 2 应支持快速模式交换，通信双方使用阶段 1 的 ISAKMP SA 协商建立 IPsec SA，IPsec SA 是为保护它们之间的数据通信而使用的策略及密钥。

本节用到的符号如下：

HDR：表示 ISAKMP 头。

HDR * ：表示 ISAKMP 头之后的载荷是加密的。

SA：带有一个或多个建议载荷的安全关联载荷。

IDi：发起方的标识载荷。

IDr：响应方的标识载荷。

HASH：HASH 载荷。

HASH_I：发起方的 HASH 载荷。

HASH_R：响应方的 HASH 载荷。

SIG_I：发起方的签名载荷。

SIG_R：响应方的签名载荷。

CERT：证书载荷。

CERT-I：发起方的证书载荷。

CERT-R：响应方的证书载荷。

KE：密钥交换载荷，包含 Diffie-Hellman 密钥交换的公开值。

Ni：发起方的 Nonce 载荷。

Nr：响应方的 Nonce 载荷。

〈P〉_b：载荷〈P〉的数据部分，不包含 ISAKMP 的通用头部。

PubKey_i：发起方的公钥。

PubKey_r：响应方的公钥。

CKY-I：初始方的 Cookie。

CKY-R：响应方的 Cookie。

VID：销售商 ID。

MAC：消息认证码，用于验证报文的完整性。

Prf：伪随机函数。通常是通信双方协商好的 HASH 函数的一个 HMAC（HASH 消息认证代码，是密码意义上更加强壮的用 HASH 函数计算 MAC 的方法）版本。

[x]：x 是可选的。

〈x〉y：用密钥 y 对 x 进行加密。

B.2 密钥交换机制

B.2.1 阶段 1 主模式交换

B.2.1.1 预共享密钥认证交换

预共享密钥认证的主模式交换过程由 6 条消息组成，交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SA	⟶	
2		⟵	HDR,SA
3	HDR,KE,Ni	⟶	
4		⟵	HDR,KE,Nr
5	HDR*,IDi,HASH_I	⟶	
6		⟵	HDR*,IDr,HASH_R

消息 1 和消息 2，发起方向响应方发送一个封装有建议载荷的安全关联载荷，而建议载荷中又封装有变换载荷。响应方接受到该消息后，同样发送一个安全关联载荷，在载荷中表明它所接受的发起方发送的 SA 建议。

消息 3 和消息 4，发起方和响应方交换数据，交换的数据内容包括密钥交换载荷、nonce 载荷。密钥交换载荷包含 Diffie-Hellman 密钥交换的公开值，用于生成密钥材料。此时通信双方还没有完成身份认证。

消息 5 和消息 6，发起方和响应方交换身份信息并对交换过程进行认证。这两条消息中传递的内容使用前面协商的算法和密钥加密保护。

B.2.1.2 数字签名认证交换

数字签名认证的主模式阶段 1 交换的消息序列如下：

消息序列	发起方	方向	响应方
1	HDR,SA	⟶	
2		⟵	HDR,SA
3	HDR,KE,Ni	⟶	
4		⟵	HDR,KE,Nr
5	HDR*,IDi,[CERT,] SIG_I	⟶	
6		⟵	HDR*,IDr,[CERT,] SIG_R

数字签名认证交换的前 4 条消息功能与预共享密钥认证交换的前 4 条消息相同。

消息 5 和消息 6，通信双方对彼此身份进行验证。SIG_I 及 SIG_R 分别是发起方和响应方应用自己的私钥对 HASH_I 和 HASH_R 签名的结果。

B.2.1.3 公钥加密认证交换

公钥加密认证的主模式阶段 1 交换的消息序列如下：

消息序列	发起方	方向	响应方
1	HDR,SA	⟶	
2		⟵	HDR,SA
3	HDR,KE,[HASH(1),] 〈IDi_b〉PubKey_r,〈Ni_b〉PubKey_r	⟶	

4		←	HDR,KE,〈IDr_b〉PubKey_i, 〈Nr_b〉PubKey_i
5	HDR*,HASH_I	→	
6		←	HDR*,HASH_R

消息 1 和消息 2 的功能与预共享密钥认证交换中的前 2 条消息相同。

消息 3,发起方将所使用公钥证书的 HASH 值(即 HASH(1))传递给响应方,便于响应方确定用哪个证书对应的私钥对被加密的载荷解密。所传递的身份标识和随机数均由响应方的公钥加密。

消息 4 对响应方的身份及随机数均由发起方的公钥加密。

消息 5 和消息 6 的功能与预共享密钥认证交换中的消息 5 和消息 6 相同。

B.2.1.4 改进的公钥加密认证交换

改进的公钥加密认证的主模式阶段 1 交换的消息序列如下:

消息序列	发起方	方向	响应方
1	HDR,SA	→	
2		←	HDR,SA
3	HDR,[HASH(1),] 〈Ni_b〉PubKey_r, 〈KE_b〉Ke_i, 〈IDi_b〉Ke_i, [〈Cert-I_b〉Ke_i]	→	
4		←	HDR,〈Nr_b〉PubKey_i, 〈KE_b〉Ke_r, 〈IDr_b〉Ke_r,
5	HDR*,HASH_I	→	
6		←	HDR*,HASH_R

消息 1 和消息 2 的功能与预共享密钥认证交换中的前 2 条消息相同。

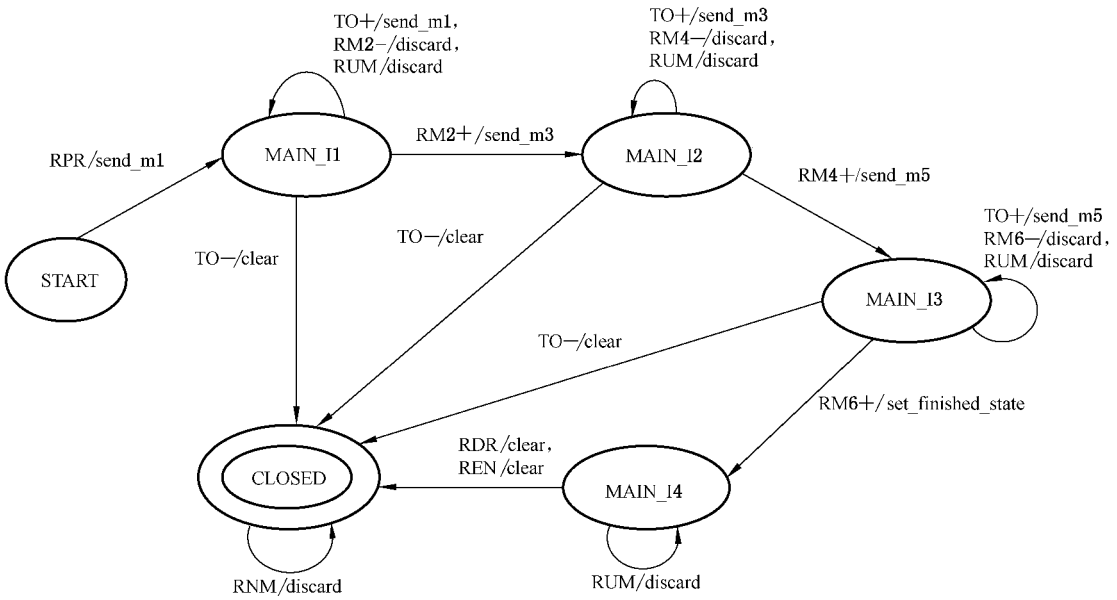
消息 3,发起方将所使用公钥证书的 HASH 值(即 HASH(1))传递给响应方,便于响应方确定用哪个证书对应的私钥对被加密的载荷解密。所传递的随机数 Nonce 载荷使用公钥加密,而密钥交换载荷、身份标识载荷均由对称密钥加密算法保证安全。

消息 4,响应方使用公钥加密算法对随机数 Nonce 载荷加密,密钥交换载荷、身份标识载荷均由对称密钥加密算法保证安全。

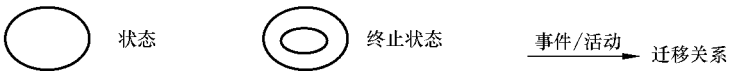
消息 5 和消息 6 的功能与预共享密钥认证交换中的消息 5 和消息 6 相同。

B.2.1.5 发起方行为

在 IKEv1 主模式交换情况下,发起方行为状态如图 B.1 所示。



说明(下同):



状态:

START:初始状态,连接尚未建立,重传计时器未运行。

MAIN_I1:已发送消息 1,等待消息 2,重传计时器运行。

MAIN_I2:已发送消息 3,等待消息 4,重传计时器运行。

MAIN_I3:已发送消息 5,等待消息 6,重传计时器运行。

MAIN_I4:已收到消息 6,阶段 1 协商完成,重传计时器未运行。

CLOSED:关闭状态,协商不成功或连接关闭,重传计时器未运行。

活动:

send_m1:发送消息 1。

send_m3:发送消息 3。

send_m5:发送消息 5。

set_finished_state:设置协商完成标志。

discard:丢弃接收到的消息。

clear:清除连接状态。

事件:

Receive_Protocol_Request(RPR):收到底层协议引擎(如 IPsec)的协商请求。

Receive_message_2(RM2+,RM2−):接收到消息 2。RM2+指示接收到的消息可接受,RM2−指示接收到的消息不可接受。

Receive_message_4(RM4+,RM4−):接收到消息 4。RM4+指示接收到的消息可接受,RM4−指示接收到的消息不可接受。

Receive_message_6(RM6+,RM6−):接收到消息 6。RM6+指示接收到的消息可接受,RM6−指示接收到的消息不可接受。

Timeout(TO+,TO−):重传计时器到期。TO+指示重传计数器大于 0,TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM):接收到非期望的消息,如 Main_I1 状态接收到消息 2 之外的其他消息。

Receive_Negotation_Message(RNM):接收到协商的消息。

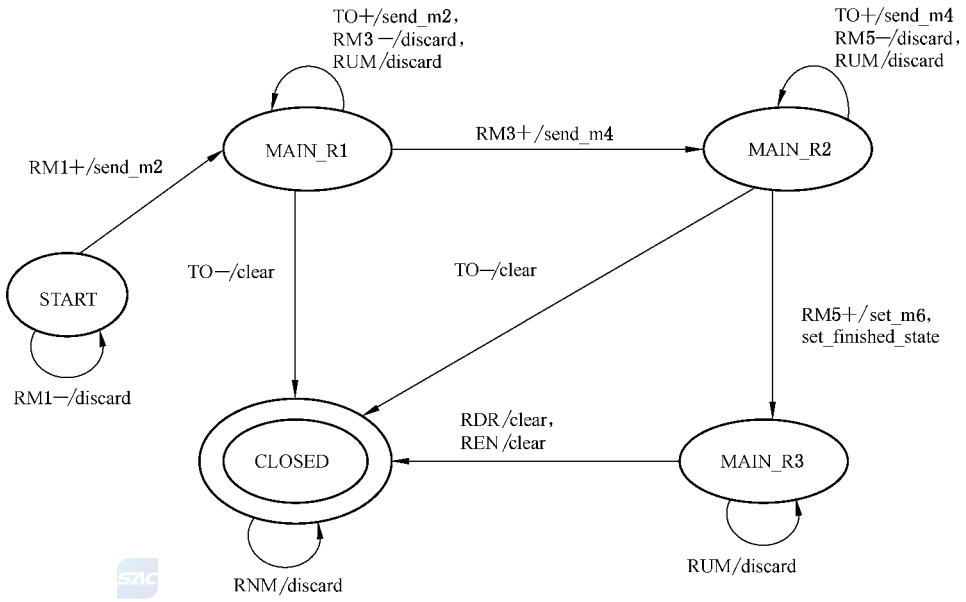
Receive_Delete_Request(RDR):接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN):接收到 ISAKMP SA 到期通知消息。

图 B.1 IKEv1 主模式交换发起方行为状态图

B.2.1.6 响应方行为

在 IKEv1 主模式交换情况下,响应方行为状态如图 B.2 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

MAIN_R1：已发送消息 2，等待消息 3，重传计时器运行。

MAIN_R2：已发送消息 4，等待消息 5，重传计时器运行。

MAIN_R3：已发送消息 6，协商完毕，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_m2：发送消息 2。

send_m4：发送消息 4。

send_m5：发送消息 6。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

Receive_message_1(RM1＋,RM1－)：接收到消息 1。RM1＋指示接收到的消息可接受，RM1－指示接收到的消息不可接受。

Receive_message_3(RM3＋,RM3－)：接收到消息 3。RM3＋指示接收到的消息可接受，RM3－指示接收到的消息不可接受。

Receive_message_5(RM5＋,RM5－)：接收到消息 5。RM5＋指示接收到的消息可接受，RM5－指示接收到的消息不可接受。

Timeout(TO＋,TO－)：重传计时器到期。TO＋指示重传计数器大于 0，TO－指示重传计数器等于 0。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 Main_R1 状态接收到消息 3 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

Receive_Delete_Request(RDR)：接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN)：接收到 ISAKMP SA 到期通知消息。

图 B.2　IKEv1 主模式交换响应方行为状态图

B.2.2　阶段 1 野蛮模式交换

B.2.2.1　预共享密钥认证交换

预共享密钥认证的野蛮模式交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SA,KE,Ni,IDi	⟶	
2		⟵	HDR,SA,KE,Nr,IDr,HASH_R
3	HDR,HASH_I	⟶	

野蛮模式使用3条消息来实现密钥交换。其中消息1和消息2协商策略，进行Diffie-Hellman密钥交换；消息2和消息3对通信双方的身份进行验证。

B.2.2.2 数字签名认证交换

数字签名认证的野蛮模式交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SA,KE,Ni,IDi	→	
2		←	HDR,SA,KE,Nr,IDr,[CERT,] SIG_R
3	HDR,[CERT,] SIG_I	→	

消息1与消息2的功能与预共享密钥认证交换的消息1和消息2相同。

消息2和消息3实现通信双方身份的验证，SIG_I及SIG_R分别是发起方和响应方应用自己的私钥对HASH_I和HASH_R签名的结果。

B.2.2.3 公钥加密认证交换

公钥加密认证的野蛮模式交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SA,[HASH(1),] KE,〈IDi_b〉PubKey_r,〈Ni_b〉PubKey_r	→	
2		←	HDR,SA,KE,〈IDr_b〉PubKey_i,〈Nr_b〉PubKey_i,HASH_R
3	HDR,HASH_I	→	

公钥加密认证的野蛮模式交换序列中，消息1和消息2实现安全关联参数协商、密钥交换、身份交换(标识载荷是加密传输的)，确保了通信双方身份的保密性。消息2和消息3实现通信双方身份的验证。

B.2.2.4 改进的公钥加密认证交换

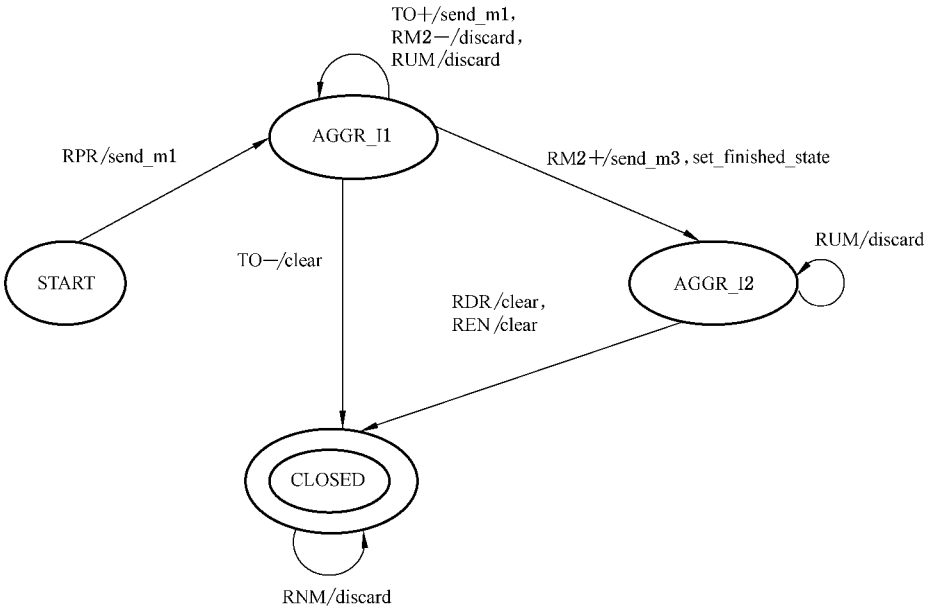
改进的公钥加密认证的野蛮模式交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SA,[HASH(1),]〈Ni_b〉PubKey_r,〈KE_b〉Ke_i,〈IDi_b〉Ke_i[,〈Cert-I_b〉Ke_i]	→	
2		←	HDR,SA,〈Nr_b〉PubKey_i,〈KE_b〉Ke_r,〈IDr_b〉Ke_r,HASH_R
3	HDR,HASH_I	→	

改进的公钥加密认证的野蛮模式交换序列中，消息1和消息2交换的功能与公钥加密认证方式相同，此外密钥交换载荷、身份标识载荷均由对称密钥加密算法保证安全。消息2和消息3实现通信双方身份的验证。

B.2.2.5 发起方行为

在 IKEv1 野蛮模式交换情况下，发起方行为状态如图 B.3 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

AGGR_I1：已发送消息 1，等待消息 2，重传计时器运行。

AGGR_I2：已发送消息 3，协商完毕，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

d_m1：发送消息 1。

send_m3：发送消息 3。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

eceive_Protocol_Request(RPR)：收到底层协议引擎(如 IPsec)的协商请求。

Receive_message_2(RM2+，RM2−)：接收到消息 2。RM2+指示接收到的消息可接受，RM2−指示接收到的消息不可接受。

Timeout(TO+，TO−)：重传计时器到期。TO+指示重传计数器大于 0，TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 AGGR_I1 状态接收到消息 2 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

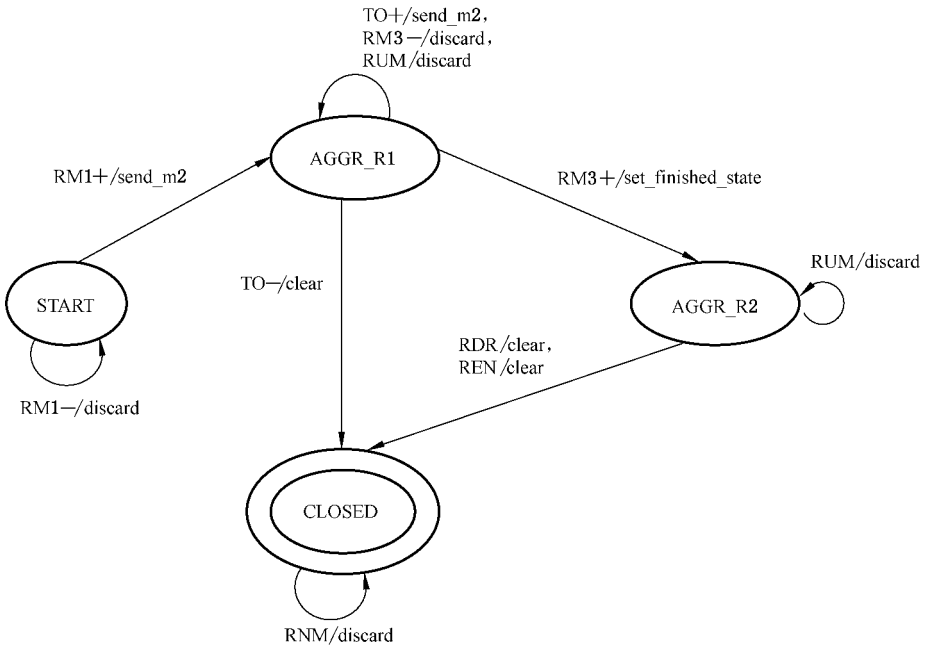
Receive_Delete_Request(RDR)：接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN)：接收到 ISAKMP SA 到期通知消息。

图 B.3 IKEv1 野蛮模式交换发起方行为状态图

B.2.2.6 响应方行为

在 IKEv1 野蛮模式交换情况下，响应方行为状态如图 B.4 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

AGGR_R1：已接收到消息 1，等待消息 3，重传计时器运行。

AGGR_R2：已接收到消息 3，协商完成，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_m2：发送消息 2。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

Receive_message_1(RM1+，RM1—)：接收到消息 1。RM1+指示接收到的消息可接受，RM1—指示接收到的消息不可接受。

Receive_message_3(RM3+，RM3—)：接收到消息 3。RM3+指示接收到的消息可接受，RM3—指示接收到的消息不可接受。

Timeout(TO+，TO—)：重传计时器到期。TO+指示重传计数器大于 0，TO—指示重传计数器等于 0。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 AGGR_R1 状态接收到消息 3 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

Receive_Delete_Request(RDR)：接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN)：接收到 ISAKMP SA 到期通知消息。

图 B.4　IKEv1 野蛮模式交换响应方行为状态图

B.2.3　阶段 2 快速模式交换

B.2.3.1　快速模式交换过程

阶段 2 的交换依赖于阶段 1 的交换。阶段 2 交换的信息由阶段 1 建立的 ISAKMP SA 保护，即除了 ISAKMP 头外所有的载荷都要加密。快速模式的交换过程如下：

消息序列	发起方	方向	响应方
1	HDR*，HASH(1)，SA，Ni [，KE] [，IDi，IDr]	⟶	
2		⟵	HDR*，HASH(2)，SA，Nr [，KE] [，IDi，IDr]
3	HDR*，HASH(3)	⟶	

消息 1,发起方向响应方发送一个 HASH 载荷、一个安全关联载荷(其中封装了一个或多个建议载荷,而每个建议载荷中又封装了一个或多个变换载荷)、一个 nonce 载荷、一个密钥交换载荷和标识载荷。

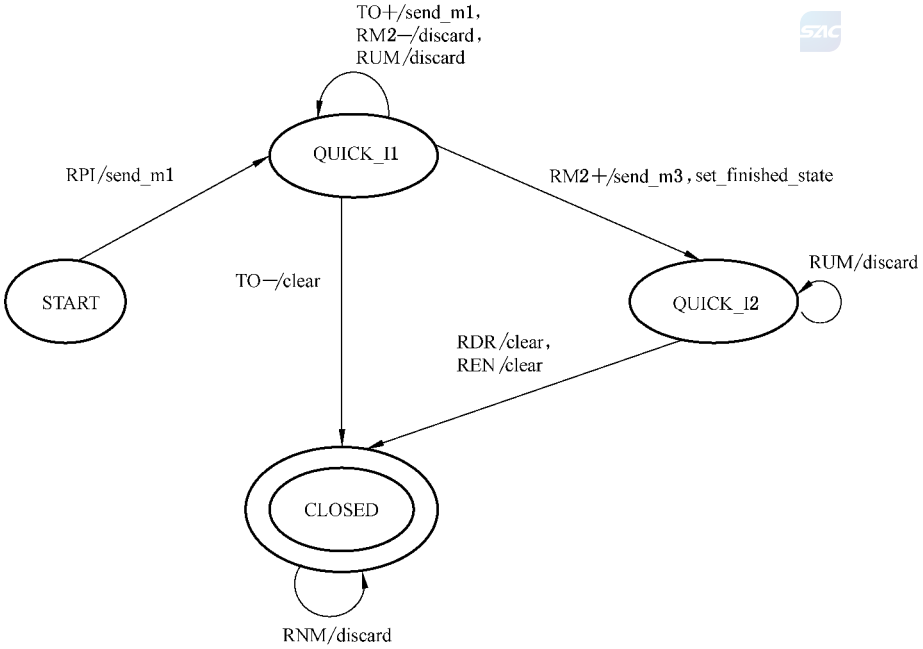
消息 2,响应方向发起方发送一个 HASH 载荷、一个安全关联载荷、一个 nonce 载荷、一个密钥交换载荷和标识载荷。

消息 3,发起方向响应方发送一个 HASH 载荷,用于对前面的交换进行认证。

上述消息交换完毕,生成会话密钥材料,用于驱动生成安全协议(如 AH 或 ESP)使用的密钥。

B.2.3.2 发起方行为

在 IKEv1 快速模式交换情况下,发起方行为状态如图 B.5 所示。



状态:

START:初始状态,连接尚未建立,重传计时器未运行。

QUICK_I1:已发送消息 1,等待消息 2,重传计时器运行。

QUICK_I2:已发送消息 3,协商完毕,重传计时器未运行。

CLOSED:关闭状态,协商不成功或连接关闭,重传计时器未运行。

活动:

send_m1:发送消息 1。

send_m3:发送消息 3。

set_finished_state:设置协商完成标志。

discard:丢弃接收到的消息。

clear:清除连接状态。

事件:

Receive_Protocol_Identification(RPI):收到阶段 1 协商完毕的指示。

Receive_message_2(RM2+,RM2−):接收到消息 2。RM2+指示接收到的消息可接受,RM2−指示接收到的消息不可接受。

Timeout(TO+,TO−):重传计时器到期。TO+指示重传计数器大于 0,TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM):接收到非期望的消息,如 QUICK_I1 状态接收到消息 2 之外的其他消息。

Receive_Negotation_Message(RNM):接收到协商的消息。

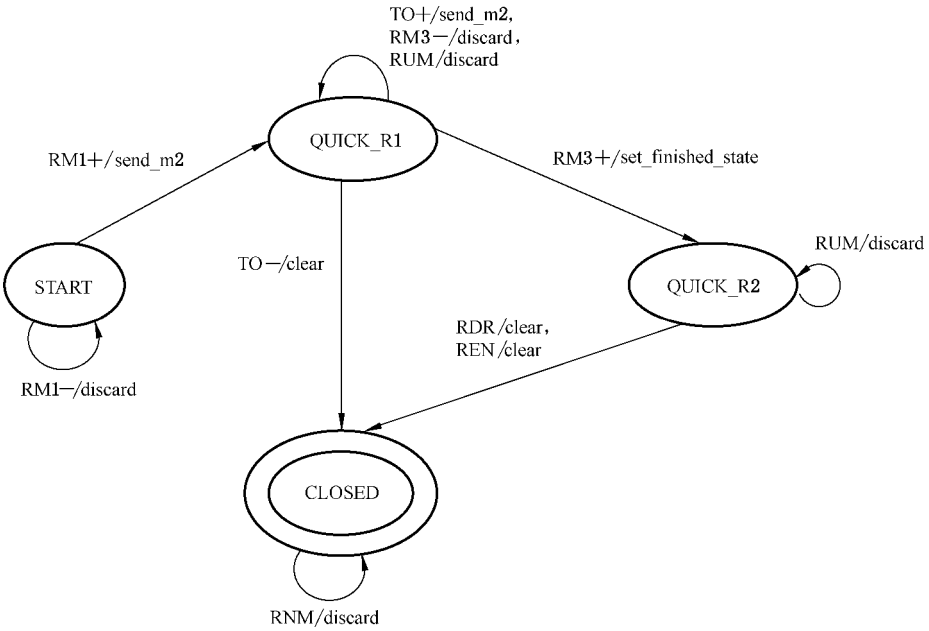
Receive_Delete_Request(RDR):接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN):接收到 ISAKMP SA 和 IPsec SA 到期通知消息。

图 B.5 IKEv1 快速模式交换发起方行为状态图

B.2.3.3 响应方行为

在 IKEv1 快速模式交换情况下，响应方行为状态如图 B.6 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

QUICK_R1：已接收到消息 1，等待消息 3，重传计时器运行。

QUICK_R2：已接收到消息 3，协商完成，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_m2：发送消息 2。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

Receive_message_1(RM1+，RM1−)：接收到消息 1。RM1+指示接收到的消息可接受，RM1−指示接收到的消息不可接受。

Receive_message_3(RM3+，RM3−)：接收到消息 3。RM3+指示接收到的消息可接受，RM3−指示接收到的消息不可接受。

Timeout(TO+，TO−)：重传计时器到期。TO+指示重传计数器大于 0，TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 AGGR_R1 状态接收到消息 3 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

Receive_Delete_Request(RDR)：接收到删除 ISAKMP SA 请求。

Receive_Expire_Notify(REN)：接收到 ISAKMP SA 和 IPsec SA 到期通知消息。

图 B.6 IKEv1 快速模式交换响应方行为状态图

B.2.4 信息交换

信息交换用于 SA 的维护和管理。通过信息交换，参与通信的双方均能向对方发送状态及错误提示消息。该消息既不需要确认，也不能担保肯定能够到达目的地。由于这种交换具有不可靠的特点，所以并不强行要求发送它。信息交换最常见的一种用途是向对方发出通知，告诉它一个特定的 SA (ISAKMP SA 或 IPsec SA)已被删除，应避免再使用它。

消息序列	发起方	方向	响应方
1	HDR*，HASH(1)，N/D	⟶	

其中 N/D 表示或者为通知载荷，或者为删除载荷。

附 录 C
（资料性附录）
IKEv2 密钥交换机制

C.1 定义

IKEv2 是 IKE 的第二个版本协议，是 IPsec 用来实施相互认证和建立、维护安全关联的组件。IKEv2 对 IKEv1 中的报文格式、载荷格式以及交换机制进行了修订，建立更为可靠的加密和验证机制。

本节用到的符号如下：

AUTH：认证载荷。

CP：配置载荷。

D：删除载荷。

E：加密载荷。

EAP：扩展认证载荷。

TSi：发起方业务选择载荷。

TSr：响应方业务选择载荷。

其他符号见 B.1 定义。

C.1 密钥交换机制

C.2.1 初始交换

C.2.1.1 初始交换过程

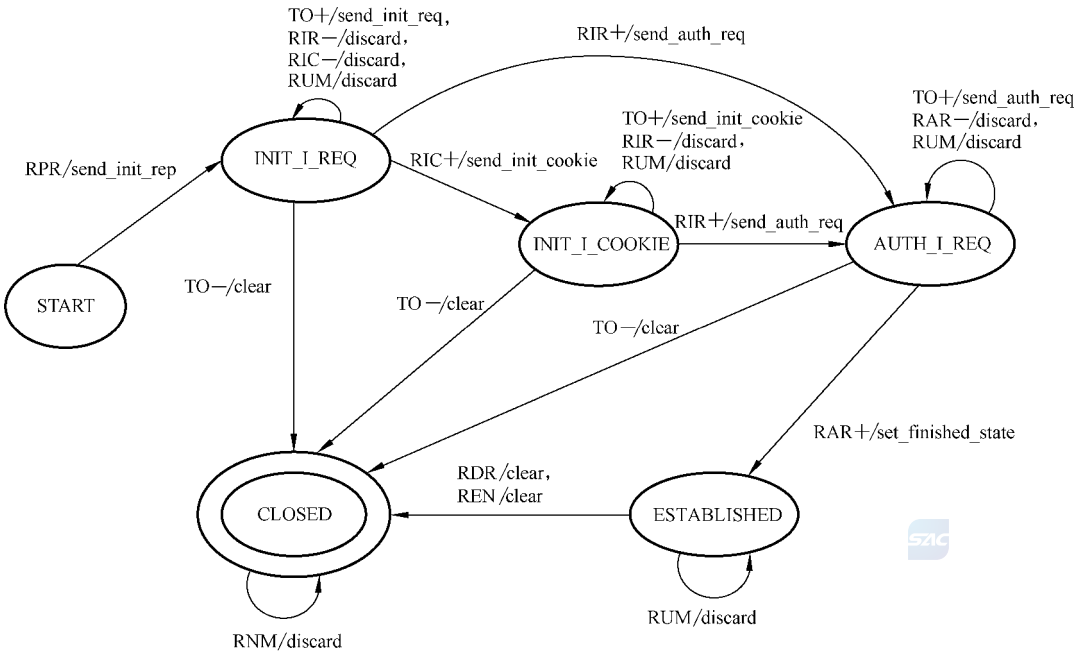
初始交换实现了 IKEv1 中阶段 1 和阶段 2 所完成的功能，用于建立 IKE SA 和 CHILD SA（即 IPsec SA）。在 IKEv2 中身份认证方法仅使用了数字签名和预共享密钥等，两种认证方式使用相同的消息交换格式，初始交换流程如下：

消息序列	发起方	方向	响应方
1	HDR,SAi1,KEi,Ni	⟶	
2		⟵	HDR,SAr1,KEr,Nr,[CERTREQ]
3	HDR,SK {IDi,[CERT,] [CERTREQ,] [IDr,] AUTH,SAi2,TSi,TSr}	⟶	
4		⟵	HDR,SK {IDr,[CERT,] AUTH, SAr2,TSi,TSr}

初始交换由 4 条消息组成。在 IKEv2 中的消息都是成对出现的，初始交换的前面 2 条消息称为 IKE_SA_INIT 交换，用于密钥算法的协商、Nonce 交换以及一次共享密钥的交换，从而用于生成加密和验证后续交换的密钥材料。后 2 条消息称为 IKE_AUTH 交换，用于认证前面交换的消息，同时交换身份和证书信息，并建立第一个 CHILD SA，除了消息头外，IKE_AUTH 交换中的消息都由前面协商生成的算法和密钥进行加密和完整性保护。

C.2.1.2 发起方行为

在 IKEv2 初始交换情况下，发起方行为状态如图 C.1 所示：



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

INIT_I_REQ：已发送 INIT 请求，等待响应，重传计时器运行。

INIT_I_COOKIE：已发送带 Cookie 的请求，等待响应，重传计时器运行。

AUTH_I_REQ：已发送 AUTH 请求，等待响应，重传计时器运行。

ESTABLISHED：已收到 AUTH 响应，协商完成，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_init_req：发送 init 请求消息。

send_init_cookie：发送带 Cookie 的 init 请求消息。

send_auth_req：发送 auth 请求消息。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

Receive_Protocol_Request(RPR)：收到底层协议引擎(如 IPsec)的协商请求。

Receive_Init_Res(RIR+，RIR−)：接收到 INIT 响应消息。RIR+指示接收到的消息可接受，RIR−指示接收到的消息不可接受。

Receive_Init_Cookie(RIC+，RIC−)：接收到带 Cookie 的响应消息。RIC+指示接收到的消息可接受，RIC−指示接收到的消息不可接受。

Receive_Auth_Res(RAR+，RAR−)：接收到认证响应消息。RAR+指示接收到的消息可接受，RAR−指示接收到的消息不可接受。

Timeout(TO+，TO−)：重传计时器到期。TO+指示重传计数器大于 0，TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 INIT_I_REQ 状态接收到 RIR 和 RIC 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

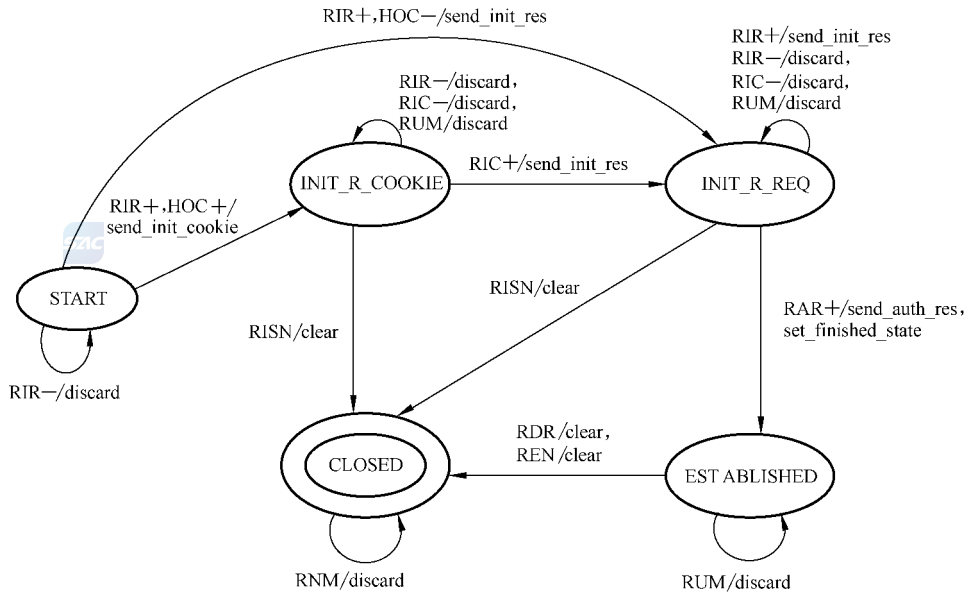
Receive_Delete_Request(RDR)：接收到删除 IKE SA 请求。

Receive_Expire_Notify(REN)：接收到 IKE SA 到期通知消息。

图 C.1　IKEv2 初始交换发起方行为状态图

C.2.1.3　响应方行为

在 IKEv2 初始交换情况下，响应方行为状态如图 C.2 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

INIT_R_REQ：已发送 INIT 响应，等待 AUTH 请求，重传计时器运行。

INIT_R_COOKIE：已发送带 Cookie 的请求，等待响应，重传计时器运行。

ESTABLISHED：已发送 AUTH 响应，协商完成，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_init_res：发送 init 响应消息。

send_init_cookie：发送带 Cookie 的通知消息。

send_auth_res：发送 auth 响应消息。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态

事件：

Receive_Init_Req(RIR+，RIR−)：接收到 INIT 请求消息。RIR+指示接收到的消息可接受，RIR−指示接收到的消息不可接受。

Receive_Init_Cookie(RIC+，RIC−)：接收到带 Cookie 的 INIT 请求消息。RIC+指示接收到的消息可接受，RIC−指示接收到的消息不可接受。

Receive_Auth_Req(RAR+，RAR−)：接收到认证请求消息。RAR+指示接收到的消息可接受，RAR−指示接收到的消息不可接受。

Receive_Invalid_Syntax_Notify(RISN)：接收到 INVALID SYNTAX 通知。

Half_Open_Count(HOC+，HOC−)：当前的半打开连接数目。HOC+指示半打开连接数目达到门限值，HOC−指示未达到门限值。

Receive_unexpected_message(RUM)：接收到非期望的消息，如在 INIT_R_REQ 状态西接收到 RIR、RIC 和 RAR 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

Receive_Delete_Request(RDR)：接收到删除 IKE SA 请求。

Receive_Expire_Notify(REN)：接收到 IKE SA 到期通知消息。

图 C.2　IKEv2 初始交换响应方行为状态图

C.2.2　创建子 SA 交换

C.2.2.1　创建子 SA 交换过程

创建子 SA 交换是 IKEv2 的阶段 2，可为 IPsec 协议（如 AH、ESP）协商相关参数，可支持 PFS 功能。创建子 SA 交换流程如下：

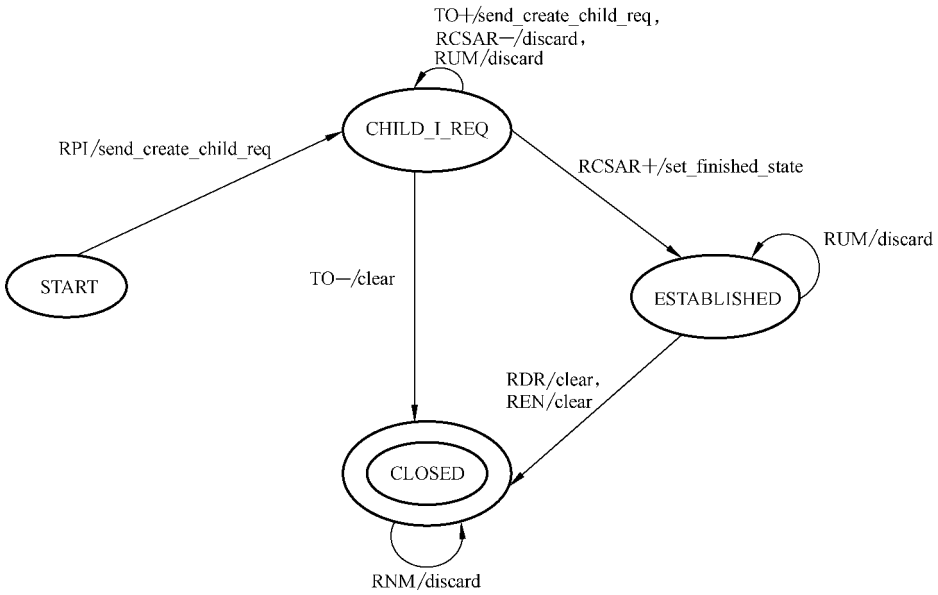
消息序列	发起方	方向	响应方
1	HDR,SK {[N],SA,Ni,[KEi],[TSi,TSr]}	⟶	
2		⟵	HDR,SK {SA,Nr,[KEr],[TSi,TSr]}

创建子 SA 交换包含两条消息,第一条消息发送 SA 提案,交换 Nonce 和流量选择符;第二条消息对 SA 提案和流量选择符进行响应,交换 Nonce。根据是否支持 PFS 功能,可提供密钥交换载荷 KE。

利用创建子 SA 可进行密钥等参数的更新。若交换的消息中不提供业务流选择载荷,则可用于更新 IKE SA 的相关参数;若提供,则用于更新 IPsec SA 的参数。可由 N 载荷中提供的安全参数索引值 SPI 指明更新的 SA。

C.2.2.2 发起方行为

在 IKEv2 创建子 SA 交换情况下,发起方行为状态如图 C.3 所示:



状态:

START:初始状态,连接尚未建立,重传计时器未运行。

CHILD_I_REQ:已发送创建 CHILD SA 请求,等待响应,重传计时器运行。

ESTABLISHED:已收到创建 CHILD SA 响应,协商完成,重传计时器未运行。

CLOSED:关闭状态,协商不成功或连接关闭,重传计时器未运行。

活动:

send_create_child_req:发送 init 请求消息。

set_finished_state:设置协商完成标志。

discard:丢弃接收到的消息。

clear:清除连接状态。

事件:

Receive_Protocol_Identification(RPI):收到安全协议的协商指示。

Receive_Child_SA_Res(RCSAR+,RCSAR−):接收到创建 Child_SA 响应消息。RCSAR+指示接收到的消息可接受,RCSAR−指示接收到的消息不可接受。

Timeout(TO+,TO−):重传计时器到期。TO+指示重传计数器大于 0,TO−指示重传计数器等于 0。

Receive_unexpected_message(RUM):接收到非期望的消息,如 CHILD_I_REQ 状态接收到 RCSAR 之外的其他消息。

Receive_Negotation_Message(RNM):接收到协商的消息。

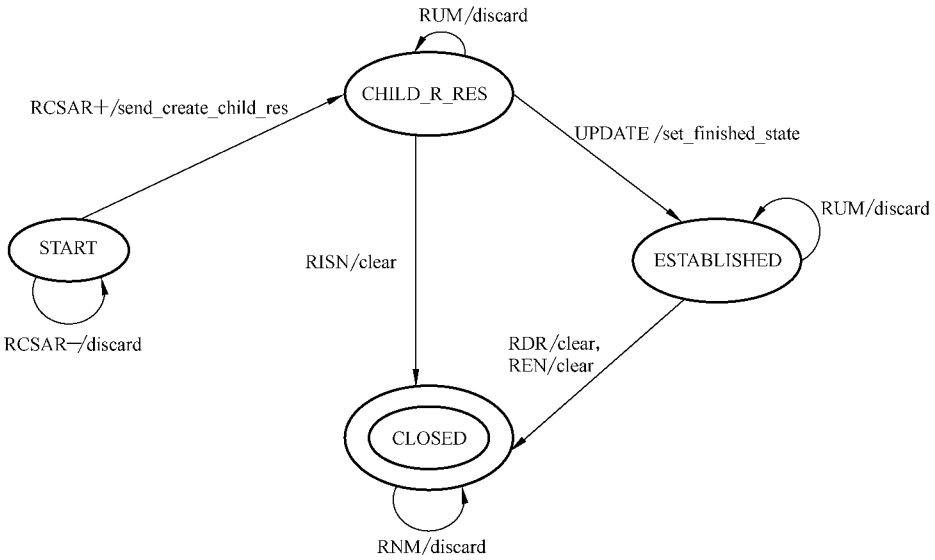
Receive_Delete_Request(RDR):接收到删除 IKE SA 请求。

Receive_Expire_Notify(REN):接收到 IKE SA 到期通知消息。

图 C.3 IKEv2 创建 CHILD SA 交换发起方行为状态图

C.2.2.3 响应方行为

在 IKEv2 创建子 SA 交换情况下，响应方行为状态如图 C.4 所示。



状态：

START：初始状态，连接尚未建立，重传计时器未运行。

CHILD_R_RES：已收到创建 CHILD SA 请求，返回响应，重传计时器未运行。

ESTABLISHED：参数更新完毕，协商完成，重传计时器未运行。

CLOSED：关闭状态，协商不成功或连接关闭，重传计时器未运行。

活动：

send_create_child_res：发送 init 响应消息。

set_finished_state：设置协商完成标志。

discard：丢弃接收到的消息。

clear：清除连接状态。

事件：

Receive_Child_SA_Req(RCSAR+，RCSAR−)：接收到创建 Child_SA 请求消息。RCSAR+指示接收到的消息可接受，RCSAR−指示接收到的消息不可接受。

UPDATE：计算密钥，更新参数。

Receive_Invalid_Syntax_Notify(RISN)：接收到 INVALID SYNTAX 通知。

Receive_unexpected_message(RUM)：接收到非期望的消息，如 START 状态接收到 RCSAR 之外的其他消息。

Receive_Negotation_Message(RNM)：接收到协商的消息。

Receive_Delete_Request(RDR)：接收到删除 IKE SA 请求。

Receive_Expire_Notify(REN)：接收到 IKE SA 到期通知消息。

图 C.4 IKEv2 创建 CHILD SA 交换响应方行为状态图

C.2.3 信息交换

通信双方在密钥协商期间，需要传送控制消息，告知对方发生的错误或者通知某些事件。为了完成此操作，IKEv2 定义了消息交换。消息交换过程可以包含多个通知载荷、删除载荷和配置载荷，同第一版不同，对方收到消息后必须作出响应。消息交换必须在进行初始化交换后进行，并且消息的内容也要经过加密。信息交换流程如下：

消息序列	发起方	方向	响应方
1	HDR，SK {[N，][D，][CP，]...}	⟶	
2		⟵	HDR，SK {[N，][D，][CP]，...}

参 考 文 献

[1] RFC791 因特网协议(Internet Protocol)

[2] RFC792 因特网控制报文协议(Internet Control Message Protocol)

[3] RFC2407 因特网安全关联和密钥管理协议(ISAKMP)的 IP 安全解释域 (The Internet IP Security Domain of Interpretation for ISAKMP)

[4] RFC2408 因特网安全关联和密钥管理协议(Internet Security Association and Key Management Protocol (ISAKMP))

[5] RFC2409 因特网密钥交换协议(The Internet Key Exchange (IKE))

[6] RFC3715 IPsec—NAT 的兼容性要求(IPsec-Network Address Translation (NAT) Compatibility Requirements)

[7] RFC3947 IKE 中 NAT 穿越协商(Negotiation of NAT—Traversal in the IKE)

[8] RFC3948 IPsec 封装安全载荷(ESP)报文的 UDP 封装(UDP Encapsulation of IPsec ESP Packets)

[9] RFC4301 因特网协议安全体系(Security Architecture for the Internet Protocol)

[10] RFC4302 IP 认证头协议(IP Authentication Header)

[11] RFC4303 IP 封装安全载荷协议(IP Encapsulating Security Payload (ESP))

[12] RFC4306 因特网密钥交换协议版本 2(Internet Key Exchange (IKEv2) Protocol)

[13] IPsec VPN 技术规范,国家密码管理局发布,2008 年 1 月

中 华 人 民 共 和 国
国 家 标 准
IPsec 协议应用测试规范
GB/T 28456—2012
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-68522006
2012 年 10 月第一版
*
书号:155066·1-45611

GB/T 28456-2012